AD-A286 837

ATION PAGE

Form Approved
OMB No. 0704-0188

...average 1 hour per response, including the time for reviewing instructions, searching existing data sources, ...ng the collection of information. Send comments regarding this burden estimate or any other aspect of this ... to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson ...of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	30 JAN 1995	FINAL - V 1.0

4. TITLE AND SUBTITLE
Department of Defense Goal Security Architecture (DGSA) Transition Plan

5. FUNDING NUMBERS
C - MDA904-93-C-B054

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
DGSA Core Team
c/o Edward Rothenheber
Suite 150
891 Elkridge Landing Rd.
Linthicum, MD 21090

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Center for Information Systems Security
Architecture + Engineering
Director, NSA
Attn: X13/CISS A+E (Russ Flowers)
Fort George G. Meade, MD 20755-6000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES Field 25 should contain the identifier CIM (Collection), as detailed in A. Washington DTIC-OCS 10M, 4/11/94.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Public

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

14. SUBJECT TERMS
DGSA, TRANSITION PLAN, TAFIM, SECURITY

15. NUMBER OF PAGES
136

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

NSN 7540-01-280-5500
Standard Form 298 (Rev 2-89)
Prescribed by ANSI Std 239-18
298-102

POC ED ROTHENHEBER 410-684-6488

13. ABSTRACT

"Transition to the Department of Defense (DoD) Goal Security Architecture (DGSA) [1] is defined as the incorporation of DGSA-specified security concepts into information systems through system development and modernization efforts, focused on making the achievement of the DGSA security vision possible. The DGSA provides the goal and objectives, while this plan identifies a path to achievement in incremental steps and accomplishable tasking. With well over 7000 major information systems within the DoD, addressing those individual systems within this transition plan would be an impossible task. Therefore, this plan presents a uniform approach for the migration of information systems toward the DGSA common security goal. The plan's focus leads to enhanced information system security that is responsive to potential threats, flexible in its administration, interoperable in its execution, standard in its structure, and affordable.

1.1 Purpose

This DGSA transition plan is intended for system planners and managers addressing security in new information system development or modernization programs. It may also be used by commercial developers, vendors, and those interested in incorporating specific security initiatives or objectives outlined in this plan into their product developments or security programs. This plan is also the mechanism for providing and maintaining coordination among the responsible organizations and those incorporating, developing, or participating in the objectives of this DGSA transition plan.

ABSTRACT

Department of Defense
Goal Security Architecture (DGSA)

Transition Plan

Version 1.0

Center for Information Systems Security
Defense Information System Security Program

Note: All comments concerning its content and applicability should be addressed through the DGSA Core Team, Attn.: Edward Rothenheber, BA&H, 891 Elkridge Landing Rd, Suite 150, Linthicum, MD 21090 or DGSATeam@bah.com. Please reply no later than 15 March 1995.

30 January 1995

(This page is intentionally blank.)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

Transition to the Department of Defense (DoD) Goal Security Architecture (DGSA) [1] is defined as the incorporation of DGSA-specified security concepts into information systems through system development and modernization efforts, focused on making the achievement of the DGSA security vision possible. The DGSA provides the goal and objectives, while this plan identifies a path to achievement in incremental steps and accomplishable tasking. With well over 7000 major information systems within the DoD, addressing those individual systems within this transition plan would be an impossible task. Therefore, this plan presents a uniform approach for the migration of information systems toward the DGSA common security goal. The plan's focus leads to enhanced information system security that is responsive to potential threats, flexible in its administration, interoperable in its execution, standard in its structure, and affordable.

1.1 Purpose

This DGSA transition plan is intended for system planners and managers addressing security in new information system development or modernization programs. It may also be used by commercial developers, vendors, and those interested in incorporating specific security initiatives or objectives outlined in this plan into their product developments or security programs. This plan is also the mechanism for providing and maintaining coordination among the responsible organizations and those incorporating, developing, or participating in the objectives of this DGSA transition plan.

The purpose of this document is not to educate the reader on the principles and the concepts of the DGSA. The reader is referred to the DGSA to gain an understanding of the principles and concepts of the DGSA. Throughout this document terms such as DGSA-consistent and DGSA-based are used; these terms signify that something is consistent with or based on the principles and concepts of the DGSA.

1.2 Scope

This goal driven plan formalizes the necessary direction, coordination, and guidance in nine interdependent security related areas. It encourages efforts that are consistent with the DGSA, and the use of Commercial-Off-The-Shelf (COTS) products. The plan provides direction and guidance to achieve DGSA security principles and objectives for incorporation into system specific architectures. It is not an architectural implementation of the DGSA, since that will vary depending upon the mission, policy, and system involved. It is applicable to both the DoD and commercial communities.

The scope of this plan encompasses nine key DGSA transition areas. These areas are termed "segments" and will be addressed separately in this document. The primary basis for this entire plan relies on the information contained in the nine segment areas. These nine segments were selected based upon their applicability in addressing all the necessary security objectives of the DGSA. While each of these segments are individually discussed and has its own strategy and relationship for the attainment of the DGSA, they are not independent. Each strategy describes such items as transition approaches, identification of tasks, staffing requirements, and the inter-task dependencies. Not all of the identified tasks and staffing requirements represent new activities. Existing efforts which support the transition to the DGSA have been included in this plan.

Section 2 provides a perspective on the major events, special considerations, forecasts, risks, schedules, and milestones for the nine segments. This provides a focus for system planners and managers when decisions must be made in planning the security direction for developments

nd modernization efforts. The individual segment strategies are found in Sections 3 through 11. Additional documents such as the DGSA or the Defense Information System Security Policy (DISSP.SP1) may be found through electronic sources or by contacting the Center for Information Systems Security (CISS) at DISA.

1.3 Background

The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence (ASD/(C3I)) initiated a set of investigations and analyses to determine how DoD could achieve an integrated, comprehensive, and economical Defense-wide Information Systems Security Program (DISSP). The results of those investigations and analyses detailed eight major objectives to provide the security requirements necessary for DoD information systems to be mission effective, interoperable, secure, and affordable. These eight objectives addressed 1) Architecture, 2) Transition Planning, 3) Security Policy, 4) Standards and Protocols, 5) Technology, 6) Accreditation Procedures, 7) Organization Improvement, and 8) Product and Service Availability. The Defense Information Systems Agency (DISA) and the National Security Agency (NSA) established a DISSP program office with joint staffing under the DISA Center for Information System Security (CISS) to achieve the eight major security objectives.

The CISS developed the DGSA and incorporated it into DoD's Technical Architecture Framework for Information Management (TAFIM) as Volume Six. The evolution of DoD information systems will be guided by the TAFIM, which defines the services, standards, high-level concepts, components, and configurations that can be used to develop architectures to satisfy specific mission requirements. As part of the TAFIM, the DGSA meets the broad security requirements of the Defense Information System. The TAFIM provides the medium for pursuing a uniform security direction. The ASD/C3I will require that new DoD information systems development and modernization programs conform to the TAFIM.

This DGSA Transition Plan satisfies the second DISSP objective by providing a continuous and dynamic transition process, but also encompasses key aspects of the other six DISSP objective areas. Its primary focus is to present a uniform incremental approach to achieving the security vision of the DGSA.

1.4 Updates to the Transition Plan

This plan will be a "living" document. It will change as the transition toward the DGSA occurs. Changes in the time frame specified for the accomplishment of DGSA objectives may occur and will be reflected through periodic update. These changes will be initiated based on monitoring the transition process, accomplishment of the defined tasks, new technologies, developments, products, and key advances toward the attainment of the DGSA goals and objectives. The majority of such changes can be anticipated to occur in the details of this transition plan (i.e., the segment strategies). The DGSA core team will be responsible for monitoring and updating this transition plan. The CISS will be responsible for identifying and coordinating the resources for the continual updating of this document.

Information received that may alter the current state of the DGSA transition will be reviewed for potential incorporation into this plan. The status of each of the nine segment areas will therefore be continually monitored by the DGSA core team and updated as required. Updated releases of the DGSA Transition Plan are scheduled to occur annually. Each newly released version of this plan will receive a new version number. Any updates deemed to be time critical may be distributed as a pre-release note or publication. Such notes will be incorporated into the next released version of the document. Each release will be reviewed to ensure that any organizational changes necessitated will be reflected accordingly. These releases will be available through the Defense Technical Information Center in both electronic and paper media.

2. OVERVIEW OF TRANSITION

The DGSA Transition Strategy organizes the transition into nine segments. Each segment represents an important element in realizing the DGSA. The nine segments are: Policy, Research and Technology (R&T), Security Management (SM), Communication Networks (CN), Standards, Products, Local Subscriber Environment (LSE), Education and Training (E&T), and Certification and Accreditation (C&A). This section presents an overview of the transition based on the information contained within the segment transition plans. This section is not intended to give a complete description of the transition, but rather to capture the important stages in the migration of the DoD information systems to DGSA-based architectures.

2.1 Transition Segments

Each of the nine segment areas has a specific purpose and focus.

Policy Segment -- transition and consolidation of DoD security policies to enable DGSA-consistent information systems implementations.

R&T Segment -- create DGSA-supporting technologies and influence the initiation or continuation of programs proving the DGSA concepts.

SM Segment -- ensure the availability of DGSA-consistent security management resources, including technology, devices, standards, training, and frameworks.

CN Segment -- reduce dependence on DoD-unique communications networks, and maximize the use of common carrier networks.

Products Segment -- assess existing and planned products for DGSA consistency.

LSE Segment -- provide information system program managers with DGSA-related standards, products, and research and technology information; develop planning strategies for transition toward the DGSA goals.

Standards Segment -- promote the availability of security-related standards to support the DGSA.

E&T Segment -- promote the DGSA transition process by developing instruction on the security policies, DGSA architecture, concepts, technologies, and implementations.

C&A Segment -- develop a process consistent with the DGSA-principles for assessing system security implementations in fielded systems and approving their operation.

Each of the nine segments possesses an inherent dependency on the tasking of each of the other segments. Every task in a segment transition strategy identifies the task's reliance on the inputs from other tasks and identifies which other tasks are dependent upon this task's outputs. The following paragraphs present a high level discussion on the interdependency of the segments. More detailed discussions can be found in the segment transition strategies.

The tasking proposed across all the segments represents a major investment of resources by the DoD. If it were necessary to identify new resources for the entire range of tasks, it would be unrealistic to believe the transition could be achievable, fortunately, this is not necessary. There are a significant number of existing activities in different DoD organizations that are

satisfying some of the transition tasks using existing resources. These activities are included in this transition plan.

The policy segment will work with the other segments to enable DGSA-consistent information systems implementations. The policy segment will receive the results of R&T tasks intended to simulate or implement the DGSA concepts, and to provide proof of the concepts viability for information systems security. The policy segment will obtain policy recommendations from the CN segment for dealing with Traffic Flow Security (TFS) and availability. The CN contributions will be used by the policy segment to develop guidance for TFS and availability policies. These policy guidance documents will support the development of training materials under E&T tasks. The policy segment establishes policy as the requirements support the metrics that determine C&A accomplishment. The structure of the policy provides the basis for the process and structure of C&A, which cannot proceed without documented policy guidance.

In the mid and long terms, all of the other segments are reliant upon the R&T segment activities. New approaches to security will emerge from R&T activities. R&T will also provide technologies that will enable desired security policies to be implemented effectively.

The SM segment will prototype the elements of security management, such as Security Management Application Processes (SMAP), a Security Association Management Protocol (SAMP) protocol, and security management operating system elements. SM will define roles and relationships of users and security administrators and the policy elements required to accomplish their mission for the LSE segment. In coordination with the CN segment, SM will define the relationship between managers of information systems and managers of communications networks. SM needs standards involving security policy parameters, Security Management Information Base (SMIB) data objects and attributes, and security protocols such as SAMP from the Standards segment. SM defines and produces several guidance documents and tools for further implementation which must be incorporated into E&T material. SM activities result in essential ingredients for establishing a uniform process for C&A, through the establishment of uniform metrics for security mechanisms.

The CN and LSE segments are closely associated. The LSE segment must satisfy the mission security needs without reliance on security elements being placed within the communications network. The CN segment will convey the perceived user needs for CN security management to the SM segment. The CN segment will coordinate closely with the Products and R&T segments with respect to availability criteria for LSE and communications products. The CN segment will also coordinate with the Standards segment in order to determine the impact of the approval of various related standards.

By its nature the LSE segment impacts every other segment. The LSE segment is tasked with identifying the security requirements of the thirteen functional areas within DoD. The LSE segment transition approach calls for the development of a process whereby the requirements of the system security architects can be transformed into products.

The Standards development process should deal with emerging technology trends so that standards will be available when vendors begin to develop products to implement these emerging technologies. The dependency on emerging technology will be fulfilled by information from R&T. The SM segment will be providing the foundation for development of a number of new standards. Information on the availability of standards based products, especially de facto standards, that can influence the standards development process will be provided by the Products segment. The use and benefits of standards will be incorporated in E&T material.

The E&T segment team requires interaction with all of the segment teams. All areas of the DGSA addressed by the segment teams require E&T module development. Initially, educational materials focusing on the DGSA and its concepts are necessary. As the DGSA transition process gains momentum, training materials on the transition process will also be required.

The C&A segment will employ the results of all other segment teams to determine compliance with policy. An open distributed environment will require new policies, philosophies, and innovative techniques to meet the needs of the DGSA. When implemented, new C&A policies will provide a systematic approach for determining the security posture across an open distributed architecture, per the DGSA concepts. The C&A segment is essentially dependent on all other segments within the DGSA transition process. As a result, the success of applying a new C&A process for the DGSA will be a measure of how well all segments within the transition process are integrated. The issues that are encountered by certifiers and accreditors during implementation will reflect any shortcomings in the transition approaches of all segments. Through the interactions of the segment teams and the transition core team, this information will be reflected in updates to the tasking of the individual segment transition strategies.

2.2 Milestones

Each segment area has identified key milestones in its segment strategy. These milestones do not necessarily coincide with a specific task contained within a segment strategy. They may also represent the completion of a body of work or attainment of a specific segment goal. The milestones signify progress for a segment in realizing the concepts and principles of the DGSA. Figure 2-1 charts the integration of transition milestones for each segment. The integrated milestone chart can be used to assist program managers in DGSA transition planning. Modernization or developmental efforts may be planned during the life cycle of a program. The initial phase of the program life cycle, from planned initiation to implementation, is defined as the program transition window. Program managers can use the integrated milestone chart to examine the key project segment results that occur during a particular program transition window. For example, if a program's transition window corresponds to the 1998-99 time frame, the program manager can recognize that there are significant milestones being reached in seven of the nine segments. DGSA consistent products will be available, according to the Products Segment, as well as the security management infrastructure. The program manager will also see that connectivity is still provided through the DoD networks, since the communication networks segment milestone for common carrier connectivity does not occur until 2000. By placing the segment milestones within the perspective of a program's transition window, the program manager will be able to effectively plan the program's transition to the DGSA.

2.3 Interim States

In viewing the integrated milestone chart, it becomes apparent that there are significant points in the transition due to the realization of a group of milestones. These points are identified as interim states. The first point occurs in 1995 and represents the baseline in the transition. Transition strategies for each of the nine segment areas will have been initiated and a basis for transitioning each segment area will have been established. The first interim state will occur in 1997 and corresponds to the development of the separation technology prototypes. Separation technology is the foundation for the architecture. The next interim state will occur in 2000 and represents the achievement of DGSA-consistent migration systems. This represents the institutionalization of the concepts and principles of the DGSA in the evolution of DoD information systems. The next interim state will occur in 2005 and signifies the completion of the DGSA infrastructure. At this time all of the tasking identified in this plan will be complete and COTS-based end systems will be implemented or available to provide the security envisioned within the DGSA.

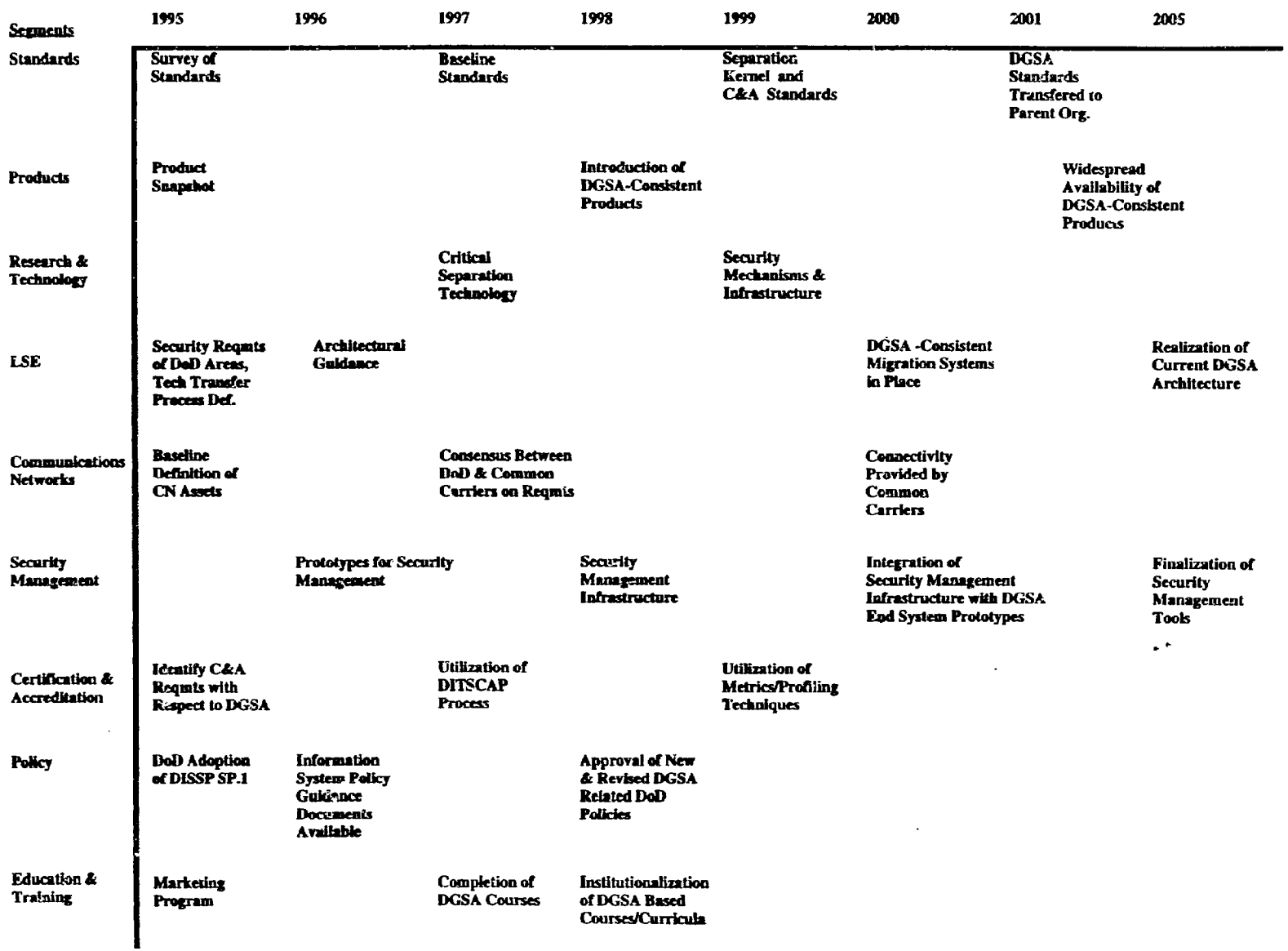


Figure 2-1. Integrated Milestone Chart

2.3.1 Baseline (1995)

The baseline state defines the key transition activities that are being accomplished in 1995. As shown in Figure 2-1, those activities are the survey of standards, product snapshot, security requirements of the DoD functional areas, technology transfer process definition, baseline definition of the communication networks assets, identification of the certification and accreditation requirements with respect to the DGSA, adoption of DISSP-SP.1, and the initiation of the marketing program. The achievement of these milestones will provide a foundation for the transition to the DGSA.

The most critical milestone is the adoption of DISSP-SP.1. DISSP-SP.1 is the foundation of the DGSA. This milestone provides the basis for a significant portion of the activities of the other segments. This policy has been approved by the DISSP Security Policy Working Group (SPWG), but needs to be formally adopted by the DoD.

A successful migration to the DGSA requires both its understanding and wide acceptance by the DoD, other Federal, and commercial communities. To facilitate this, a marketing effort will be initiated to educate these communities on the concepts and benefits of the DGSA. Successful completion of the education and awareness program is a significant milestone since it signifies that the DGSA concepts and benefits have been communicated to those communities.

A successful transition requires that information systems are designed using the concepts and principles of the DGSA. This requires that guidance on the development of a DGSA-based architecture be available and products to support a given architecture be identified. The products snapshot, along with the architectural guidance provided by the LSE segment, will provide the necessary support to architects as they begin to transition their systems.

Currently, products are not available which can satisfy all of the requirements outlined in the DGSA. The remaining milestones focus on providing the basis for obtaining the necessary products. These activities include refining DoD security requirements for specific functional areas, surveying the state of the standards activities, and initiating a process whereby the requirements can result in COTS products.

2.3.2 Critical Separation Technology (1997)

The next interim state occurs in the 1997 time frame. At this point in the transition, the foundation for the implementation of architectures which utilize the principles and concepts of the DGSA within their local subscriber environments will have been established. The milestones achieved by the end of 1997 are the baseline standards, separation technology prototypes, architectural guidance, consensus between the DoD and the common carriers on communication requirements, prototypes for security management, use of the new C&A process, information system policy guidance documents, and completion of the DGSA course materials.

This interim state's most critical milestone is the achievement of the separation technology prototypes. Separation technology is the framework for the implementation of security within end systems. The integration of the security management prototypes, the baseline standards, and the separation technology prototypes provide the basis for the development of high assurance end systems, where security services are invoked through the applications and operating system, required by the DGSA. The combination of these milestones represents a significant stage in the transition to the DGSA.

The focus of the remaining milestones is providing support to the professionals in the community who will be responsible for transitioning to the DGSA. Course materials will be

completed, so training on the DGSA can be initiated both on the architecture and how to apply the architecture. Guidance documents will be available on developing policies and architectures based on the DGSA. The new certification and accreditation policy will be utilized simplifying and standardizing that process. Achievement and consensus between the DoD and the common carriers will allow program managers to rely on common carriers to provide their connectivity.

The completion of these milestones provides a critical mass for the migration to DGSA based local subscriber environments. At the conclusion of this interim state, all of the significant pieces will be available to develop end systems which incorporate the concepts and principles of the DGSA. The focus of future transition activities will be the integration of these pieces into a prototype end system.

2.3.3 DGSA-Consistent Migration Systems (2000)

This interim state represents a significant migration to a DGSA-based environment. COTS products are becoming available which have integrated the separation technology with the security management infrastructure enabling the development of DGSA-consistent migration systems. The milestones that have been realized at this point are separation kernel and C&A standards, introduction of DGSA-consistent products, security management infrastructure, DGSA-consistent migration systems in place, security mechanisms and infrastructure, connectivity provided by common carriers, integration of security management infrastructure with DGSA end system prototypes, utilization of metrics and profiling techniques, approval of new and revised DGSA related DoD policies, and institutionalization of DGSA based courses and curricula. The realization of this interim state represents a complete foundation for the transition of the DoD to DGSA-consistent LSEs. By the year 2000, the necessary critical mass will exist to transition DoD information systems to a DGSA-based environment.

2.3.4 DGSA Infrastructure Completion (2005)

The DGSA is intended to be a mutable goal in that, as the fundamental security requirements and technology change, the DGSA will change. This "completion" state represents the realization of the DGSA as it is defined today. At this point, all standards activities required by the DGSA will have become institutionalized by parent organizations. Products that are based on the principles embodied in the DGSA will be available and in wide use. Such products include end systems which will instantiate and enforce multiple security policies. Primarily, security will be provided by these end systems and common carriers will provide connectivity between LSEs. Security management tools will be available to assist in the instantiation of the security policies within the end systems.

2.4 Critical Tasks

Within each segment area, there are critical activities that must be successfully pursued to ensure the success of the overall DGSA transition process. These activities are represented by critical tasks identified and discussed within each segment area.

In the Policy Segment, a critical task requires the revision of existing policies to address the requirements of DISSP SP.1 and the DGSA. All DGSA-related tasks extending beyond FY94 may be impacted by Task 1 of the Policy Segment. Task 1 involves adoption of the requirements of DISSP-SP.1. That is, the requirements need to be reflected either in existing DoD policy documents of in a new set of DoD policy documents. DISSP-SP.1 requirements lay the groundwork for acceptance of the DGSA. Approval of the SP.1 requirements will ensure the continued DGSA-related task funding.

The Research and Technology Segment area contains three critical activities: separation kernel development, security management information base development, and key management infrastructure development. The separation kernel development activity is represented by four development subtasks: separation kernel, security contexts, security associations, and other security critical functions. These activities taken together reflect, the elementary research and development activities that must be initiated to prove the concepts of the DGSA and to demonstrate the desired separation technology functionality. The results of these tasks will provide a basis for COTS products vendors to develop future separation technology products.

The Security Management Segment also has three critical activities: development of the SMAP, development of the supporting security infrastructure, and development of the security management protocols and standards. Like the Research and Technology activities, the results of these tasks will provide the basis for COTS products vendors to develop future security management products, that support scalable system implementations.

The Standards Segment area contains two critical activities: support for the development of separation kernel standards and support for the development of security management standards consistent with the DGSA. Separation kernel standards are critical to ensuring a measure of uniformity for the interfaces to separation kernels and available guidance for the design and implementation of separation kernels. Security management standards are critical for ensuring uniformity and standardization of the security management protocols and objects, and providing uniformity for security management protocols, objects, and security management registration activities.

The critical activity in the Products Segment involves the assessment of current products and those for the near-term and far-term. This activity is critical to ensuring that system planners and developers have access to reliable information regarding product capability and availability. As the development activities of Research and Technology and Security Management are completed and the results obtained by vendors for use in products, information about the vendors and their intended products will be added to the product assessments. The assessments may also be used by vendors to determine product overlap or duplication and aid in determining potential market share.

The critical activity undertaken by the LSE Segment is the development of process definitions guidance. This task establishes the process to transfer new technologies from R&T to the vendor community for the DGSA transition. The technology transfer process will define how the DGSA architectural requirements will be transitioned into COTS products. The assessments from the critical products activity will aid in the initial development of this guidance.

There are four critical activities in the Education and Training Segment area: DGSA and transition marketing, publication of papers on the DGSA and transition, development of an overview educational course on the DGSA and transition, and modification of existing security and technology courses to accommodate the DGSA. The modifications to existing courses will include a section discussing the technology transfer process developed under the LSE critical activities. Courses will also be modified to teach the concepts of the DGSA and describe its transition process. These courses are critical for establishing a knowledgeable work force and ensuring that the DGSA concepts and its transition process are understood. The remaining three critical tasks of the Education and Training Segment will establish an initial foundation for acceptance of the DGSA in the DoD, the security technology community, and among commercial vendors. The marketing efforts and overview educational course will be geared to the DoD and commercial vendors, while the technical papers will be focused for the academic and technical community. These activities will ensure that all participants in the DGSA

transition process have a common foundation and a vested interest in the success of that process.

In the Communication Networks Segment, a critical task requires the definition and specification of availability criteria. Availability criteria is not adequately stated for vendors to easily understand the requirements, the Government consistently evaluated systems based on the requirements. This task will ensure that the DGSA requirement for availability can be understood and satisfied by commercial carriers.

In the Certification and Accreditation Segment, a critical task requires development and documentation of a new process for Certification and Accreditation (C&A). This new C&A process will ensure that the accreditation of information domains for DGSA-consistent systems will be uniform and support a reduction of the costs involved in C&A through the reuse of accreditation results.

2.5 Risk Areas

The three main high risk areas for DGSA transition are: development of the separation kernel technology, commercial vendor acceptance of the DGSA concepts, and the costs associated with security management. For these areas, risk mitigation strategies have been established. Although not all risk can be eliminated, measures can be pursued to address the risk. Such risk mitigation strategies are intended to prevent serious schedule setbacks and preclude unplanned resource allocations.

There are no guarantees that the result of any given research and development activity will satisfy the requirements upon which the activity was based. In addition, results from the separation kernel research and development might not satisfy the desired efficiency and cost criteria. One of the highest risk elements of this transition plan is the development of separation technology that is suitable for supporting the DGSA concepts. This technology will include separation kernels, information domain support, security contexts and associations, and a suitable infrastructure.

To address the risk associated with separation technology development, a separate subtask in the Research and Technology Segment strategy was established. This subtask requires the exploration of alternatives to separation kernels. The results of this subtask will identify other technological paths and provide recommendations with respect to additional tasks needed to provide alternatives should the separation kernel approach not be viable.

Once the separation technology has been developed, acceptance by commercial vendors is required. Commercial vendors will need to believe that separation technology will be desired by their customers. In addition, commercial vendors will need to be convinced that the technologies developed will not detrimentally impact their product lines and that a market will exist beyond the DoD. The separation technology will need to be transferred free of charge to the COTS product vendors. The technology transfer process will need to ensure that vendors' development and use of the separation technology coincides with the DoD requirements. Lack of commercial vendors' acceptance of the technology would lead to insufficient quantities of products, resulting in higher costs for specialized technology.

Multiple strategies will be pursued to gain acceptance of the DGSA by both the DoD and commercial communities. DoD adoption of the DISSP SP.1 will ensure that DoD will focus on the DGSA. To gain further acceptance of the DoD and community at large, a marketing effort will be initiated. This effort requires promotion of the DGSA concepts and technologies in all communities of interest (e.g., DoD, technology vendors, DoD contractors, commercial industry). In addition, specific tasks have been identified in the Research and Technology and Standards

Segment transition strategies that will solicit the participation of major commercial vendors. Finally, the LSE Segment transition strategy describes a task to develop a technology transfer process that will involve the vendor community throughout the transition process and beyond. Successful promotion of the DGSA and vendor participation will increase the likelihood of vendor acceptance of the technology.

In the past, the security management of systems has been a cost driver. This has been due to the lack of an appropriate scalable security management infrastructure, inadequate and sometimes non-existent tools for security management and administration, and the need for specialized personnel . An appropriate security management infrastructure should be developed. Such an infrastructure will improve the productivity of security managers, thus reducing the manpower costs. Ownership and operation of the infrastructure (e.g., key management) are the real cost drivers. Tools that ease the burden on the end user must be available to support security management and administration. Future tools will need to adequately and effectively handle the complexities of technology and address distributed security management. Inability to provide such tools will result in lack of acceptance by the end user community.

To address the cost risk associated with security management, a significant task has been identified in the Security Management portion of this transition plan for the development of a cost-effective security management infrastructure. This infrastructure will leverage off of the existing security management infrastructure elements, such as Electronic Key Management System (EKMS), and planned infrastructures, such as that being developed for Defense Messaging System (DMS). The Security Management activities of this transition plan also identify several tasks that are specifically oriented to the development of useful security management tools. Such developments, particularly if the LSE-developed vendor technology transfer process noted above is successful, should provide cost-effective tools that will be necessary for effective distributed security management.

(This page is intentionally blank.)

3. POLICY SEGMENT TRANSITION STRATEGY

3.1 Introduction

Security policies referred to in this strategy are those concerned with the protection of information while it is being managed in the performance of the missions of the DoD. Such policies give guidance to users, administrators, developers, certifiers, and accreditors of information management systems. The scope of such policies as they are discussed here range from U. S. national policies to the policies of individual Government employees.

Unlike the other segments, the policy segment does not derive its direction from the DGSA. The initiatives planned here and the DGSA are both driven by the security objectives of the DoD community. This strategy addresses security policy initiatives that will make the transition of DoD information systems toward the DGSA possible. The DGSA was founded on a new approach to system security with new concepts for achieving the security objectives of the DoD community. Policy revision was called for in the DISSP Action Plan [4] which was a major source of these security objectives. An analysis of the state of information systems, the desired operational capabilities, and the requirements for protection was accomplished in accordance with the DISSP Action Plan and was documented by the DISSP as DISSP-SP.1. That policy was approved in June 1992 by the DISSP SPWG as the basis for a DISSP effort in security architecture. Following minor revisions in February 1993, this policy is now referred to as DISSP-SP.1.

The recommendations of the DISSP-SP.1 were summarized in Section 2.1 of the DGSA. They are:

- DoD information systems must support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information.
- DoD information systems must be sufficiently protected to allow distributed information processing (including distributed information system management) among multiple hosts on multiple networks in accordance with open systems architectures.
- DoD information systems must support information processing among users with different security attributes employing resources with varying degrees of security protection, including users of nonsecure resources if a particular mission so dictates.
- DoD information systems must be sufficiently protected to allow connectivity to common carrier (public) communications systems.

In addition to setting security objectives, DISSP-SP.1 defined several concepts which are derived from mission and security objectives. The most important of these are information domains, strict isolation, and absolute protection. These were incorporated directly into the DGSA and are explained in Section 4 of that document. The DGSA includes the allocation of security services that meet the objectives and defines a model for security management in open, distributed information systems.

Prior to the DISSP-SP.1 there was no policy recognition of the stated security objectives of the DoD community. Prior to the DGSA there was no recommended approach for achieving those objectives. The DISSP-SP.1 and the DGSA are the only policy and architecture offered to

guide DoD in providing the desired security in the development of its mission specific information systems.

3.2 Background

The most important existing policy regarding security in information systems for the DoD is embodied in two documents; DoD Directive 5200.28 [5], Security Requirements for Automated Information Systems (AISs), and DoD 5200.5, Communications Security (COMSEC). The first document focuses on computer security (COMPUSEC) and contains early attempts at addressing system security. The second document, as the title indicates, deals only with COMSEC. Under COMPUSEC, Public Law (PL) 100-235, The Computer Security Act, and 10 USC Article 2135, The Warner Amendment to PL 100-235 are also significant. There are many policies governing the management of classified information but they are not germane to this transition strategy.

At the recommendation of a Joint (DoD and Central Intelligence Agency) (CIA) Security Commission (JSC) a Policy Forum of DoD, CIA, and other Federal Agencies was formed to address security policy needs. A report [6] was issued by the JSC with recommendations concerning the protection of both classified and unclassified information.

The past practice of providing independent policy for COMPUSEC and COMSEC has been a road block to progress in system security. Policy for systems must cause all information security disciplines to be combined effectively. Existing policy has been ineffective in bringing about the security products and methods to deal with current or future systems. Also, current policy has focused almost entirely on classified information when the largest body of information needing protection is unclassified. There is no existing policy which guides the organization and protection of such information.

The DISSP-SP.1 and the DGSA were produced for the purpose of bringing about necessary changes in system security. The DISSP-SP.1 defines concepts for organizing information and security policies that will enable future systems to satisfy a much broader range of missions and functions with adequate security. The DGSA guides the development of mission-specific architectures that follow the concepts of DISSP-SP.1. Both documents foster a process of defining protection requirements as part of mission requirements, as part of defining the information management functions, and as part of defining system requirements. The essence of this segment is to initiate those actions which will move DoD in the new direction and guide system developers through this process.

3.3 Transition Approach

The initiatives in this segment must bring about changes in existing policies at all levels of the Government, from national policies to the policies of individuals. The initiatives must produce the guidance necessary to develop the new policies needed for missions, information domains, and systems. Policy will need to be developed to address the necessity for and implementation of traffic flow security, as well as guidance for a uniform certification and accreditation process.

Transition can only be achieved through convincing policy makers that the concepts of the DGSA are viable. This can only be done in conjunction with the support of the other segments. Policy makers must be educated to the concepts. They must see the accomplishment of the proof-of-concepts. They must see success through improvements to system security. Within this segment however, the principle activities must be in the production of new or modified policies and in the production of documents that will guide those involved.

The major recommendations of the policy segment are: (1) adoption of DISSP-SP.1 concepts by DoD, (2) preparation of new or modified DoD policy consistent with DISSP SP.1, and (3) the preparation of guidance documents for the development of information domain, mission, and system security policies. Where possible the segments will leverage off of existing activities, such as the National Security Agency (NSA) Information System Security Policy (ISSP) Draft Guidance, to achieve the goals of the segments.

There are two major transition points within the Policy Segment: (1) the publication of modifications or replacements for DoD Directive 5200.28 and DoD Directive 5200.5, and (2) the publication and initiation of new policy guidance documents.

3.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 3.4.6. Subsection 3.4.7 provides the status of each segment task.

3.4.1 Task 1: DISSP-SP.1 Adoption

Description: This security policy established the security requirements for the DGSA. The policy needs further coordination throughout the DoD in conjunction with the DGSA. The principles, security concepts and objectives in the policy should be reflected in other DoD and Director of Central Intelligence Directives (DCIDs) and security policy guidelines (i.e., input to task 2) which affect DoD missions.

Responsible Organization: Primary: CISS P3RM. Support: CISS A&E, ASD C3I, J6 & SECDEF staff.

Inter-task Dependencies:	Input Dependencies SM Task 1	Output Dependencies N/A
Required Staffing:	6 staff months 1994	

3.4.2 Task 2: Revisions To Existing Policies

Description: The DISSP action plan stated that DoD security policies are out of date and do not address the open and distributed nature of today's information management systems. DoD Directives 5200.5 and 5200.28 need serious revision. The revised or replacement documents must also reflect changes to Executive Order (EO) 12356 [7], Military Operational Procedures (MOPs), and Director of Central Intelligence Directives (DCIDs). All revised policies should support the contents of DISSP-SP.1. Transition to the DGSA cannot proceed effectively without DISSP-SP.1 reflection in revised policies.

Responsible Organization: Primary: SECDEF staff, ASD C3I, and the Joint Staff (J6). Support: MILDEPS, CISS P3RM.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	CN	Subtask 4.2
			E&T	Task 10
			LSE	Task 3,7

Required Staffing:	30 staff months	1994
	66 staff months	1995
	78 staff months	1996
Total	174 staff months	

3.4.3 Task 3: TFS Policy Development

Description: Traffic Flow Security (TFS) is the most expensive security service. DoD must provide policy guidance that will simplify decisions on when to apply TFS. From the TFS white paper generated by CN segment subtask 3.1 and recommended policy generated from the CN segment workplan, policy makers will develop a document specifying broad based TFS policy guidance to all of DoD. This TFS policy should specify the conditions under which full period confidentiality mechanisms must be used to provide TFS. It should also give guidance on methods of determining and coordinating specific mission TFS needs which are not covered by the DoD specific conditions. It is anticipated that DoD policy makers will request assistance from the Intelligence Operations Security (OPSEC) community to develop a broad based DoD TFS policy. The resulting policy could have significant impact on NSA link encryption product development program planning. DoD TFS policy will indicate the extent of the need for high speed bulk, link encryptors.

Responsible Organization: Primary: ASD C3I, J6, MILDEPs, NSA and other Intelligence OPSEC organizations. Support: DISA CISS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	CN	Subtask 3.2
	CN	Subtask 3.1	E&T	Task 10

Required Staffing:	3 staff months	1994
	6 staff months	1995
Total	9 staff months	

3.4.4 Task 4: Uniform Accreditation Guidance

Description: The purpose of this task is to document the recommended information management structures, methods, and criteria for achieving uniformity of policy enforcement between any two or more LSEs claiming to support common security policy. This guidance specification will document the recommended organizational structures and qualification procedures, to include training and authorization for certifiers and accreditors.

Responsible Organization. Primary: ASD C3I and J6. Support: CISS P3RM, EC&A, and A&E, MILDEPs, and all other DoD agencies.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	CN	Subtask 4.2
	C&A	Subtask 3.1	E&T	Task 10
			STD	Subtask 5.3

Required Staffing:	18 staff months	1994
	30 staff months	1995
Total	48 staff months	

3.4.5 Task 5: New Policy Guidance

This task will complete the activity of providing guidance on the preparation of security policies for missions, information domains, and systems. This task involves the preparation of source or index documents for International, National, and Organizational security policies. The task is composed of three subtasks.

Subtask 5.1: Mission Specific Security Policy Guidance

Description: This task will provide specific security policy guidance for the three mission areas: Command and Control (C2), Intelligence, and General Business. Although labeled specific security policy, the policies developed for each of the DoD mission areas will still be high level, but specifically address the particular requirements of each of the mission areas, including information transfer security requirements between the three mission areas, the mission areas and treaty organizations and other allies, the mission areas and civil Government departments, agencies, and organizations, and between the mission areas and the public. The mission area managers will lead this task, with support from DISA CISS, Center for Architecture (CFA) and individual Military Department (MILDEP) representatives. The completed mission area security policies will be reviewed by ASD C3I, the Joint Staff and the Commander in Chief (CINCs) where appropriate, and concurred by the SECDEF, Chairman of the Joint Chiefs of Staff, and the MILDEP secretaries, as deemed appropriate.

Responsible Organization: Primary: Mission area managers. Support: DISA CISS, CFA and individual MILDEP representatives.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	STD	Subtask 3.2
			LSE	Tasks 3,7
			SM	Subtask 2.2

Required Staffing:	36 staff months	1995

Subtask 5.2: Information Domain Security Policy Guidance

Description: This task establishes the guidance for mission function areas to develop their own information domain security policy. The guidance will explain the minimal essential elements of every information domain security policy, how meta policies can be used/reused, how to perform threat (of intent) analysis on the information to be protected, considerations for developing inter-domain transfer rules, how to apply metrics to threat/harm (information value derivatives) and security services, how to define user privileges and how to develop security management policy for the information domain. If necessary, information domain security policy guidance will be tailored to mission specific security policy guidance, and revised DoD and DCI security policy and policy derivatives (directives, regulations, etc.).

Responsible Organization: Primary: Mission area managers. Support: DISA CISS A&E directorate, NSA system profiling organization, CISS EC&A, CISS P3RM, and DISA CFII.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	STD	Subtask 3.2
			CN	Subtask 4.2
			SM	Subtask 2.2, Task 11
			LSE	Tasks 3,7

Required Staffing:	14 staff months	1995
	14 staff months	1996
Total	28 staff months	

Subtask 5.3: System Security Policy Guidance

Description: This task will provide specific guidance on developing system security policy from the aggregated information domain security policies which must be implemented by a particular system. This guidance will define a link security services (with defined strength) together to achieve all information domain policies, and how to perform tradeoffs regarding specific security management policies. (The system security policy defined does not have to be completely achieved to realize success. Specific system constraints do not, under any circumstances, alter the information domain or system security policies.)

Responsible Organization: Primary: CISS A&E. Support: CISS P3RM, CISS EC&A.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	STD	Subtask 3.2

Required Staffing:	12 staff months	1995
	12 staff months	1996
Total	24 staff months	

3.4.6 Resource Summary and Transition Schedule

Table 3-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 3-1 shows the segment transition schedule.

	Resources Required in Staff Months			
Task	**1994**	**1995**	**1996**	**Total**
1	6			6
2	30	66	78	174
3	3	6		9
4	18	30		48
5.1		36		36
5.2		14	14	28
5.3		12	12	24
Total	57	164	104	325

Table 3-1. Policy Segment Summary of Required Staff Resources

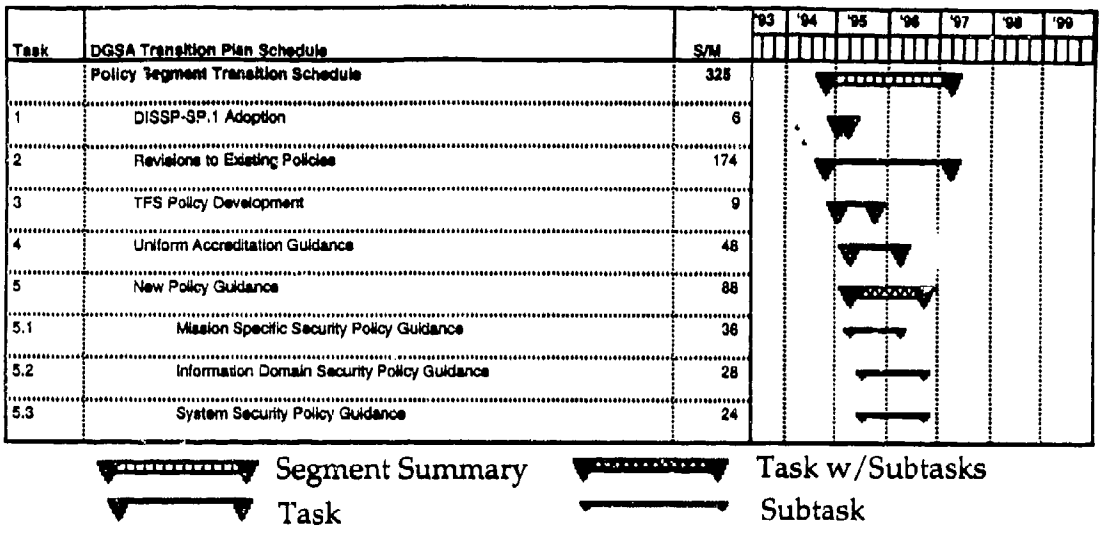


Figure 3-1 Policy Segment Transition Schedule

3.4.7 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

None of the segment tasks are being executed.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1, 2, 3, 4, 5.1, 5.2, and 5.3 have not assumed responsibility for the tasks; therefore, these tasks have not started as scheduled.

(This page is intentionally blank.)

4. RESEARCH AND TECHNOLOGY SEGMENT TRANSITION STRATEGY

4.1 Introduction

The DGSA establishes targets for security in many areas which cannot be effectively supported by current technologies. The Research and Technology (R&T) Transition Strategy provides a road map for refining and creating appropriate technology solutions that will allow future information systems to achieve the security vision of the DGSA.

The R&T segment supports the DGSA by describing the critical R&T necessary to make the architecture a reality. The purpose of this segment is (1) to identify existing DGSA-related technology efforts, and (2) to identify needed technology not covered by current programs. The transition to the goal architecture depends on available and affordable commercial products that incorporate security services. The R&T segment transition strategy is to demonstrate that technologies for information systems can be produced that achieve the DGSA targets, and then to transfer this knowledge to COTS manufacturers.

The primary goal of the R&T segment is to provide demonstrations of the essential technical parts of the DGSA. This segment is intended to marshal various Government and industry research efforts toward meeting the technical goals of the DGSA. The tasks presented in Section 4.4 are designed to create a set of evolving R&T activities that produce the essential parts of a good security basis in the short term, and move toward better and more secure solutions in the mid and long terms. A related goal is a demonstration of the DGSA concepts that will convince DoD and other users that security is available and useful without significant sacrifices in performance, cost, or maintenance. Ultimately, the goal is to convince industry that following the DGSA-related initiatives can produce information systems that are secure, function well, and are cost-competitive.

The DGSA recommendations concerning or regarding information separation require the development of separation technologies that are adequate to support simultaneous processing of information of varying sensitivities. Eventually, the technologies should support processing of that information on the same information system. In addition, the DGSA recognizes that different missions (business as well as military) have different requirements for the protection of information. This is reflected in different security policies. Today's information systems are not flexible with respect to security policies. The enforcing software derived from a security policy, once established, is not easily changed and simultaneous support for different security policies on one system generally is not feasible. The R&T development performed under this segment is aimed at allowing flexibility in establishing and enforcing security policies. Near-term development will focus on flexible single policy operation, with an evolution to multiple policies.

The DGSA also recognizes the need to have a wide range of security mechanisms to support the different security requirements expressed in mission security policies and a supporting infrastructure to manage and support those security mechanisms. Although there is continuing development of security mechanisms both within DoD and the commercial sector, the proper application of particular security mechanisms in specific situations is not well understood. When reasonable metrics for security mechanisms are available, and the security mechanisms are well matched to requirements, the ability of the security engineer to create appropriately protected information systems will be greatly enhanced. The R&T segment must respond to these requirements by undertaking activities in security mechanism metrics, in new security mechanism development where deficiencies are found, and in assuring that the infrastructure is adequate to support existing and future security mechanisms.

4.2 Background

The R&T separation technology approach is based on developing new computer operating system paradigms. Modern operating systems are very complicated, and in an effort to gain control over their development and maintenance, vendors are embracing microkernel architectures. Microkernels are attractive to industry because they consist of modules that work together in well-defined ways so that they can be modified independently of one another and independently of other parts of the information system. The microkernel approach also seeks to isolate the hardware-specific aspects of a particular platform so that portability of resulting operating systems is increased. The microkernel approach is viewed as an appropriate vehicle to implement fundamental features of the DGSA architecture, particularly the mechanisms to create the required separation of information processing, the means to apply different security policies simultaneously in a single information system, and to implement those parts of the operating system considered to be security-critical (including specific security mechanisms). Currently, most major developers of operating systems are moving toward the microkernel approach.

Another critical element of the DGSA is security management and the infrastructure it controls. Development is needed to improve the current limited capabilities for controlling and coordinating distributed security activities. A SAMP is an important part of distributed security management. Existing development efforts within NSA R2 are leading to a proof of concept protocol that will show the capabilities and limitations of competing SAMPs (such as that being produced in the Institute of Electrical & Electronic Engineers (IEEE) 802.10 committee). The proof of concept work will lead to improvements and corrections which will be offered to the appropriate standards committees.

A variety of activities exist in industry, academia, and Government research organizations to create new and better security mechanisms. These include mechanisms for user identification and authentication, access control, data integrity, data confidentiality, and availability. Unfortunately, in many instances, these efforts are uncoordinated and duplicative. In general, there is little basis on which to choose among the competing mechanisms. (When the DGSA requirement for security mechanism metrics is achieved, it will help users assess and choose mechanisms appropriate to their needs.)

One area in which activity is underway is microkernel application to security. The microkernel approach is being explored with regard to the best means to apportion security functions among software modules. The independence of security policy enforcement and security policy decisions is considered an essential division. Although, the work to date has not concentrated on simultaneous multiple security policy support, the basic mechanisms developed may be extensible. In addition, work is in progress on the implementation and evaluation of SAMP features. Related efforts in key management are also under way. Security mechanism developments in the cryptography area receive constant attention, and the application of formal methods to separation technology is being explored.

Three general difficulties must be overcome in achieving the R&T transition strategy. The first is that some of the specific technology problems to be solved are simply complex. There is no guarantee in research endeavors that setting out to solve a problem will result in a good solution in reasonable time and with available resources. For example, it simply is unknown at this time to possibly interpret all security policies with a single security policy decision function. It is also not known with any certainty that the microkernel approach to implementing information separation will produce effective and cost-efficient products. It is important to acknowledge which problems are complex and to devote sufficient resources to their solution, otherwise the results of solving easier problems may be wasted. It is also important to plan for alternative solutions for high-risk problems.

A second problem is ensuring that the solutions are sufficiently general so they can be applied to a variety of hardware platforms and vendor operating systems and applications. Because practical research can only be administered on a limited number of platforms and operating systems, it is easy to get absorbed in the detail of the research implementations and to neglect generality.

The third difficulty in achieving the R&T transition strategy will be convincing vendors that the approaches are worth their time and effort (which clearly translate to money) to adopt. In the case of operating systems vendors, this will not be easy, since (as explained in the DGSA) the approach means a fundamental restructuring of most current operating systems. The interest in microkernel architectures by vendors may go a long way toward eliminating this problem, but that remains to be seen. Even with microkernel-based operating systems, if a radically different approach to allocating functions to modules has been adopted, the use of the solutions developed through the R&T segment may be difficult to embed in those systems. Steps can be taken to encourage vendors to adopt these solutions. One is to give the technology to vendors in a form that they can embed in their products with minimal effort and expenditure. When used in products in accordance with supplied guidance, these solutions must be known to be acceptable for Government use without extensive, expensive, time-consuming evaluation. Above all, the solutions must be useful in the commercial sector so that vendors will have a market for their products.

4.3 Transition Approach

The DGSA assumes that its recommended approaches and target capabilities can only be met effectively through implementation in commercial products that are useful in the widest market place. DoD-specific solutions must be avoided if at all possible. Thus, the transition approach and the strategy of this segment is to support the development and demonstration of critical technologies, to influence standards, and to influence commercial security products. The payoff will come when the commercial sector is convinced that their large investments in communications and information technology require security safeguards, and that those safeguards can be best provided through the technologies identified and demonstrated to them that support the DGSA.

The DGSA transition requires R&T development and this strategy provides a road map toward developing short term as well as longer term solutions to technical problems. The R&T activities that are most critical are those that demonstrate the capabilities that meet the requirements of the DGSA recommendations discussed in Section 4.1. Starting with separation technology, the demonstration of these capabilities must be practical so that vendors will adopt the designs, or at least the concepts, and will provide satisfactory COTS products. These systems will evolve through further research and development to provide multiple security policy support and security mechanism selection for each security policy. The path to these capabilities includes a push and pull strategy. The push is to develop the demonstrations that prove that security can be produced without undue sacrifices in system speed and cost. The pull is to convince users, especially Government users, that they must demand and procure secure systems in their own best interests.

There are two major transition points for R&T. The first major transition point for R&T will be toward the end of 1997 or the beginning of 1998. At this time, many of the basic separation technology and security management tasks should be complete. These will provide the basis for information system products that can be used to achieve DGSA targets. Although industry should be kept abreast of the progress being made on these tasks before they are complete, it will be in this time period that complete demonstrations of the basic separation and management technologies can take place. The second major transition point will be toward the end of 1999. At this time, a significant body of knowledge will be available about security

mechanisms and the infrastructure to support them. Again, this will not all occur at once, and some of the early results should be moved to the vendors as soon as possible. However, when there is a proven range of security mechanisms, the goal of meeting security requirements wi appropriate security will be closer to being met. Other results from the R&T segment wi provide incremental improvements rather than large sudden gatherings of results. It is no possible at this time to predict when the goal of processing all sensitivities of information in a single information system will be achieved.

4.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 4.4.7. Subsection 4.4.8 provides the status of each segment task.

4.4.1 Task 1: Separation Technology

A fundamental premise of the DGSA is that end systems and relay systems must simultaneously support the activities of users in multiple information domains. This support requires that the activities administered in one information domain are independent and separate from the activities for any other information domain. The satisfaction of this requirement is critical to the success of the DGSA. The subtasks below provide the necessary technology to create a complete separation environment for practical application in commercial products.

Subtask 1.1: Separation Kernel Development

Description: The approach currently judged best for providing the required basic separation environment in end systems is the separation kernel. Many operating system vendors are using microkernels in their emerging products. Microkernels can be used to create a separation kernel environment, although not all vendors have this as a goal in their designs. Existing research projects in NSA are examining ways to include the separation kernel requirements into microkernel-based operating systems. The subtasks below describe the critical elements of separation kernels that must be created to demonstrate the viability of the approach. The R2 projects must be examined to see which of these elements are being addressed and which must be supplemented through related or new efforts.

Subtask 1.1.1: Security Policy Enforcement Function (SPEF)

Description: The SPEF is a critical part of the separation kernel. It is the mediator of all attempted actions upon resources. The SPEF responds to requests for service presented in a standard form (see Subtask 1.1.6) by obtaining a security policy decision from the Security Policy Decision Function (SPDF) (see Subtask 1.1.2) and then directing the appropriate functions to perform the requested action. This subtask should produce worked examples (including evaluation) of the basic separation kernel and the SPEF. These examples should demonstrate how to create the machine-dependent portion of a microkernel system which will be efficient and can be successfully evaluated with a minimal effort. These examples should be made available to operating system vendors for adaptation to their products. Likewise, the

results of other subtasks below should be made available to operating system vendors for porting to their products.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies	Output Dependencies	
	N/A	Prod	Subtask 1.2
		STD	Subtask 1.2

Required Staffing:		
	20 staff months	1993
	40 staff months	1994
	24 staff months	1995
	12 staff months	1996
Total	96 staff months	

Subtask 1.1.2: Security Policy Decision Function

Description: The SPDF uses parameters of a particular request for service plus information about the user making the request held in the Security Management Information Base (SMIB) to decide if the request should be carried out. This decision is made in accordance with the security policy for the information domain in which the user is operating. Given a consistent representation of the security policies the SPDF must enforce that (see subtasks 1.1.3-1.1.5), the goal of this subtask is to create a mechanism for interpreting the request parameters and SMIB information (including the security policy representation) for users operating under a wide variety of security policies at the same time. It may not be possible to create a single SPDF for all desired security policies, but the number of distinct SPDFs created should be small.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies	Output Dependencies	
	N/A	Prod	Subtask 1.2
		STD	Subtask 1.2

Required Staffing:		
	4 staff months	1993
	8 staff months	1994
	12 staff months	1995
	36 staff months	1996
	36 staff months	1997
Total	96 staff months	

Subtask 1.1.3: Security Policy Rules Representation

Description: The goal of this subtask is to create a representation scheme for security policies. This scheme must be capable of representing any desired security policy in a form that an SPDF can use effectively. Just as not every security policy might be interpretable by a single SPDF, it may be necessary to create more than one representation scheme; however, the number of such schemes should be small. Since there is essentially no experience in the area of this subtask, it may be prudent to fund parallel efforts.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
			STD	Subtasks 1.2,3.1
Required Staffing:	12 staff months	1994		
	48 staff months	1995		
	48 staff months	1996		
	36 staff months	1997		
Total	144 staff months			

Subtask 1.1.4: Information Domain Policies and Rules Prototypes

Description: The usefulness of the schemes created in subtask 1.1.3 must be judged by those who will use them. The most effective means to do this is through prototype systems. When available, the prototype systems should include the tools from Subtask 1.1.5. The experience of users with these prototype systems will provide insights for improvement of the representation schemes and the security policy rules production tools.

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
			STD	Subtask 1.2
Required Staffing:	24 staff months	1995		
	36 staff months	1996		
	36 staff months	1997		
Total	96 staff months			

Subtask 1.1.5: Tools for Security Policy Rules Production

Description: An automated tool set is required to translate information domain security policies developed by security administrators into the security policy representations developed in Subtask 1.1.3. These tools must accept the English statement of the security policy, created subject to guidance given elsewhere, and, perhaps, presented in specified paradigms. The English statement is then converted to the security policy rules representation.

Responsible Organization: DISA CISS

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
			STD	Subtask 1.2
Required Staffing:	24 staff months	1995		
	48 staff months	1996		
	24 staff months	1997		
Total	96 staff months			

Subtask 1.1.6: Standard Kernel Interface

Description: Applications that invoke operating system services do so through a set of primitive functions which are defined for a specific operating system. One of the objectives of the DGSA operating system approach is to encourage machine independence (portability) of applications

among operating systems and end system platforms that support the DGSA. By creating a single, standard set of primitive functions through which applications communicate their service requests to the SPEF, such portability can be achieved. The challenge is to encompass the different sets of primitive functions of existing (and developing) operating systems. This subtask seeks to create a satisfactory standard kernel interface. This interface must be defined with the direct involvement of technically capable representatives of all major operating system vendors. A cooperative working group approach is envisioned under the direction of the responsible organizations.

Responsible Organization: NSA, NIST

Inter-task Dependencies:	Input Dependencies	Output Dependencies	
	N/A	Prod	Subtask 1.2
		STD	Subtasks 1.1,1.2
Required Staffing:	24 staff months	1994	
	48 staff months	1995	
	24 staff months	1996	
Total	96 staff months		

Subtask 1.2: Security Contexts

Description: A security context is an instance of a user operating on an end system in a particular information domain. The security context includes, and is supported by, all applicable security mechanisms of the end system and the environment in which it operates. It is the set of security contexts, operating at any given time, that the separation mechanisms keep distinct and which are allowed to interact only in ways specified in information domain security policies. This subtask integrates the results of other subtasks as a set of functions that support actual user interactions with the separation kernel and supporting mechanisms, including security management functions.

Responsible Organization: DISA CISS/A&E, NSA R2

Inter-task Dependencies:	N/A	
Required Staffing:	12 staff months	1995
	18 staff months	1996
	18 staff months	1997
Total	48 staff months	

Subtask 1.3: Security Associations

Description: A security association provides the required protections to an application association between two security contexts (supporting the same information domain) on different end systems. Security associations are primarily a security management responsibility since agreement on and coordination of security mechanisms for information in transfer is the major aspect of security association establishment and maintenance. Prototype security association mechanisms, based on models and standards from the management and standards segments, are the product of this subtask.

Responsible Organization: DISA CISS/A&E, NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1995
	18 staff months	1996
	18 staff months	1997
Total	48 staff months	

Subtask 1.4: Other Security Critical Functions

Description: Additional security critical functions are necessary for a fully functional separation kernel-based operating system. These are discussed in some detail in the DGSA (e.g., memory management, file management, and windows management functions).

Responsible Organization: NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1994
	24 staff months	1995
	36 staff months	1996
	36 staff months	1997
Total	108 staff months	

Subtask 1.5: Formal Methods For Separation Kernel Evaluation

Description: Information domains will have differing requirements for the quality of the separation mechanisms upon which they rely. For those with the most stringent requirements, it may be possible to achieve high levels of assurance by using formal methods to evaluate separation kernel designs and implementations. This subtask will investigate the applicability of those formal methods.

Responsible Organization: NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1993
	24 staff months	1994
	24 staff months	1995
	36 staff months	1996
	36 staff months	1997
	36 staff months	1998
	36 staff months	1999
Total	204 staff months	

Subtask 1.6: Real-Time Distributed Kernel Operations

Description: The future vision for tactical information systems includes theater connectivity to all information assets. Information system platforms for forward personnel may continue to be limited, particularly in communications bandwidth and, to a lesser extent, processing power. This subtask will investigate modifications or adaptations necessary for war fighter applications of separation technology.

Responsible Organization: NSA R2, RADC

Inter-task Dependencies: N/A

Required Staffing:	36 staff months	1995
	48 staff months	1996
	48 staff months	1997
	48 staff months	1998
Total	180 staff months	

Subtask 1.7: Separation Kernel Software Evaluations

Description: Where the formal methods of subtask 1.1.5 are not applicable, evaluation techniques for separation kernel software implementations will be required. This subtask is intended to develop appropriate techniques and experience in judging "how good" a particular implementation protects and separates security contexts.

Responsible Organization: NSA C

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	60 staff months	

Subtask 1.8: Object-Oriented Technology Prototypes

Description: Object-oriented design and implementation has become a popular trend for certain applications. The proponents of object-oriented technology foresee its widespread use in a variety of applications. There are certain paradigms in the object-oriented approach that may need specialized support when melded with separation kernel implementations. This subtask will investigate the impacts of object-oriented technology and separation kernel technology on each other.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
Required Staffing:	6 staff months	1993		
	6 staff months	1994		
	24 staff months	1995		
	24 staff months	1996		
	24 staff months	1997		
	24 staff months	1998		
Total	108 staff months			

Subtask 1.9: Sponsored Product Developments

Description: This subtask is intended to be a vehicle for technology transfer to industry. As elements of separation technology near maturity, partnerships with vendors will be pursued. The eventual goal is to encourage the inclusion of DGSA-supporting technologies in COTS products.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	N/A		Prod Subtask 1.2
Required Staffing:	6 staff months	1994	
	6 staff months	1995	
	24 staff months	1996	
	36 staff months	1997	
	36 staff months	1998	
	36 staff months	1999	
Total	144 staff months		

Subtask 1.10: Alternative Separation Technologies

Description: This subtask is intended to explore alternatives to the separation kernel approach to providing information separation. Although the separation kernel approach is currently viewed as the most likely to succeed in providing the required functions, there must be preparation for alternative approaches. This task will produce a report on other technological paths to achieving the information separation required by the DGSA. The report will also make recommendations for other tasking necessary to provide a backup capability if the separation kernel approach does not succeed.

Responsible Organization: NSA R2

Inter-task Dependencies:	N/A	
Required Staffing:	24 staff months	1995
	24 staff months	1996
	18 staff months	1997
Total	66 staff months	

4.4.2 Task 2: Security Management Information Base

Security information (e.g., user attributes, security policy representations, key management information) is stored and maintained in a SMIB. There are aspects of SMIB maintenance that are not currently well-defined and which must be integrated with other parts of the end system software.

Subtask 2.1: SMIB Maintenance

Description: Facilities and tools must be defined to allow the creation, maintenance, and deletion of information domains, including enrollment of members, assigning security attributes to members, and maintaining security policy rules. This subtask will define and test methods for SMIB maintenance.

Responsible Organization: NSA R2

Inter-task Dependencies:	N/A	
Required Staffing:	24 staff months	1995
	36 staff months	1996
	36 staff months	1997
Total	96 staff months	

Subtask 2.2: SMAP/SMIB Interface

Description: The SMAP is the mechanism that applications use to invoke security services. The SMAP must make use of, create, and modify some of the information in the SMIB. An interface between the SMAP and the SMIB must be created to ensure consistency in the way SMAPs in different end systems use a distributed SMIB. This subtask will define and test a SMAP/SMIB interface.

Responsible Organization: NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
			STD	Subtasks 3.3,4.1,4.2
Required Staffing:	12 staff months	1995		
	24 staff months	1996		
	24 staff months	1997		
Total	60 staff months			

4.4.3 Task 3: Key Management Infrastructure

The success of the DGSA depends on information system interoperability. Many security mechanisms are cryptographically based. For such security mechanisms to be easily usable on a global basis, an effective electronic key management infrastructure based on international standards is essential. This task will develop techniques and procedures for management of keying material throughout its lifetime that will adequately support DoD information systems. These tasks will build on the efforts of the Electronic Key Management System (EKMS) and the Defense Messaging System (DMS).

Subtask 3.1: Information Domain/EKMS Relation Modeling

Description: This subtask identifies and solves problems associated with the EKMS and its interaction and support of the transfer of information among information domains. This subtask also considers alternatives to EKMS such as on-site key generation.

Responsible Organization: NSA R2

Inter-task Dependencies:	N/A	
Required Staffing:	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	60 staff months	

Subtask 3.2: Key Management Protocol Standards

Description: IEEE 802.10c [8] is the emerging key management standard, but has not been completely specified by the standards community. Additions to the standard may be needed to meet DoD requirements. This subtask will produce implementations of the standard to insure its proper function within the DGSA and propose amendments as necessary.

Responsible Organization: NSA R2, DISA CFS

Inter-task Dependencies:	Input Dependencies	Output Dependencies	
	N/A	Prod	Subtask 1.2
		STD	Subtask 4.4

Required Staffing:		
	12 staff months	1993
	12 staff months	1994
	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	84 staff months	

Subtask 3.3: Key Management Infrastructure Standards

Description: Key management consists of generation, storage, maintenance, update, disposal, assignment, and control of key distribution, seed key production and distribution, and physical protection of key material production and distribution. This subtask contributes to the development of standards for the key management infrastructure

Responsible Organization: Primary: DISA CFS. Support: NSA and NIST.

Inter-task Dependencies: N/A

Required Staffing:		
	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	60 staff months	

4.4.4 Task 4: Security Mechanisms

Security services are provided by invoking one or more security mechanism, such as encipherment, checksums, and authentication information validation. New or improved security mechanisms are needed to provide support to a range of security policy requirements. This task provides the basis for several such security mechanisms.

Subtask 4.1: Programmable Cryptography

Description: Programmable cryptography is the name given to microprocessor devices that perform cryptographic functions identical to their hard-wired counterparts, but are operated, controlled and configured through changes to the software. The drawback to these devices are, they may contain software "bugs" or errors, and they may be operated in ways that contravene a particular security policy. Programmable cryptographic devices are so versatile that evaluators have no tools to assess their vulnerabilities. This subtask will undertake research needed to overcome the limitations, or at least to provide means to evaluate them.

Responsible Organization: NSA R2

Inter-task Dependencies: N/A

Required Staffing:	24 staff months	1993
	48 staff months	1994
	48 staff months	1995
	48 staff months	1996
	24 staff months	1997
	12 staff months	1998
Total	204 staff months	

Subtask 4.2: Software Cryptography

Description: The easiest method of encryption is to write a software application program. NSA objects to software cryptography because anyone with access to the program can modify it or allow unauthorized reuse. If used in an inadequately protected environment, the software is highly vulnerable. This subtask will investigate means needed to protect such software.

Responsible Organization: NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1993
	30 staff months	1994
	48 staff months	1995
	48 staff months	1996
	24 staff months	1997
	12 staff months	1998
Total	174 staff months	

Subtask 4.3: Fault Detection, Fault Correction, Fault Tolerance for Security

Description: Faulty hardware or software must be detected and corrected without causing security compromises. Fault-tolerant designs must include awareness of security impacts. Fault monitoring, as it pertains to security impacts, must be accomplished as part of security management. This subtask will investigate security aspects of fault detection, correction and tolerance in an effort to enhance the basis for secure end system operations.

Responsible Organization: NSA R2

Inter-task Dependencies: N/A

Required Staffing:	36 staff months	1995
	48 staff months	1996
	24 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	132 staff months	

Subtask 4.4: Tamper Proofing

Description: Tamper proofing is used to prevent an adversary from tampering with security-critical hardware in end system components. Such components include authentication devices, audit record repositories, servers and network switches. Tamper detection devices are currently applied to specific equipments. This subtask will investigate means to apply tamper proofing techniques in more general ways and respond to new tamper proofing requirements.

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1995
	36 staff months	1996
	24 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	96 staff months	

Subtask 4.5: New Tempest Requirements And Mechanisms

Description: This task will assess the TEMPEST requirements and propose a responsible program to address those requirements. This assessment will start with the requirements in the latest version of NTISSI 7000. This subtask will create a means to determine the extent of vulnerabilities of modern equipment such as multi-user servers and switches compared to previous assessments that were performed on stand-alone and single user computer equipment.

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1995
	36 staff months	1996
	24 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	96 staff months	

Subtask 4.6: Security Mechanism Metrics

Description: Metrics are needed to characterize the relative strengths of security mechanisms so that appropriate security mechanisms can be chosen to protect information in accordance with a particular information domain security policy. Such metrics will also enable a judgment to be made about the adequacy of security mechanisms present on an end system when new information domains are created, when security policies are modified, and when end systems communicate to share information. This subtask will provide the basis for creating such metrics.

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	N/A		STD Subtasks 5.1,5.2
Required Staffing:	12 staff months	1995	
	36 staff months	1996	
	24 staff months	1997	
	12 staff months	1998	
	12 staff months	1999	
Total	96 staff months		

Subtask 4.7: Security Mechanism Catalogs

Description: Support for security architects and engineers in choosing security mechanisms to satisfy security policy requirements is needed in a manner similar to other engineering handbooks. This subtask will develop a security mechanism catalog that describes relative strengths of security mechanisms and trade-offs among them based on information developed in the previous subtask. This catalog will be integrated with the Products Database that will be developed by the Products Segment.

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies:	Input Dependencies	Output Dependencies	
	N/A	Prod	Subtask 1.2
		LSE	Task 6

Required Staffing:		
	12 staff months	1995
	36 staff months	1996
	24 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	96 staff months	

Subtask 4.8: Threat Analysis Tools

Description: Information system security architects have the responsibility for assessing the threats to particular systems in accordance with stated requirements. The threats are countered by appropriate security mechanisms. This subtask develops automated and non-automated tools to assist in threat assessment and to provide guidance in design alternatives to counter the threats. These tools will be made available to support the Certification and Accreditation Process.

Responsible Organization: DISA CISS, NSA C

Inter-task Dependencies: N/A

Required Staffing:		
	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	60 staff months	

Subtask 4.9: Vulnerability Analysis Tools

Description: Security profiles are needed to assess information system vulnerabilities. This subtask develops analysis tools to aid in the assessment of vulnerabilities and to support the choice of appropriate countermeasures. These tools will be made available to support the Certification and Accreditation process.

Responsible Organization: DISA CISS, NSA C

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
	12 staff months	1999
Total	48 staff months	

4.4.5 Task 5: Trusted Applications

The general approach in the DGSA is to avoid creating "trusted" applications since this conflicts with the ability to control and modify security policies in a single part of the SMIB. However, because of historical investments in certain trust technologies and recognizing that there may be some specialized applications in which some trust must be placed, there is a need to investigate how trusted applications can be tailored to work with and complement DGSA-consistent information system approaches. This task is intended to explore the ways trusted applications can be fit to DGSA-consistent information system architectures. (Although only one specific area is identified at this time, others may become necessary in the future.)

Subtask 5.1: Secure Database Management Systems

Description: Major development efforts have been made over several years to create secure database management systems. This subtask is to identify remaining research needs in this area and to perform the research necessary to integrate secure database management systems with DGSA-consistent architectures.

Responsible Organization: NSA R2, Rome Labs

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	N/A		Prod	Subtask 1.2
Required Staffing:	12 staff months	1995		
	12 staff months	1996		
	36 staff months	1997		
	36 staff months	1998		
	36 staff months	1999		
Total	132 staff months			

4.4.6 Task 6: Planned Improvements

Description: This task will create a review function to periodically assess the R&T segment transition strategy activities. This activity is critical to best use available R&T resources. The impact on the R&T transition strategy of changes in technology unforeseen at the time of prior reviews must be evaluated and adjustments made as necessary. Efforts that appear to be behind schedule or failing entirely must be bolstered or terminated as appropriate. Alternative approaches must be planned or instituted as required, particularly in high-risk areas (see task 1.10, for example).

Responsible Organization: DISA CISS, NSA R2

Inter-task Dependencies: N/A

Required Staffing:	6 staff months	1995
	6 staff months	1996
	6 staff months	1997
	6 staff months	1998
	6 staff months	1999
Total	30 staff months	

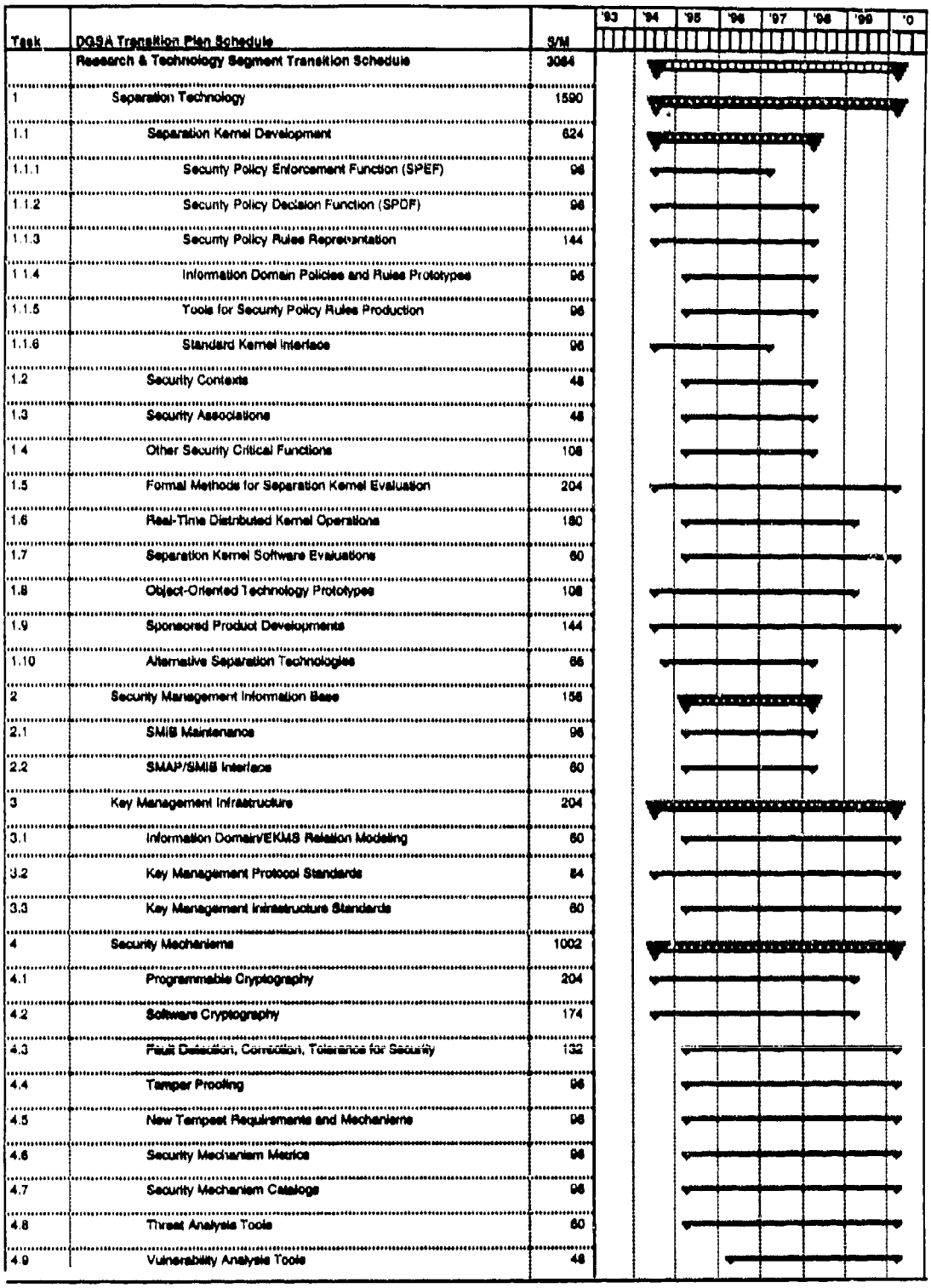
4.4.7 Resource Summary and Transition Schedule

Table 4-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 4-1 shows the segment transition schedule.

	Resources Required in Staff Months							
Tasks	1993	1994	1995	1996	1997	1998	1999	Total
1.1.1	20	40	24	12				96
1.1.2	4	8	12	36	36			96
1.1.3		12	48	48	36			144
1.1.4			24	36	36			96
1.1.5			24	48	24			96
1.2			12	18	18			48
1.3			12	18	18			48
1.4		12	24	36	36			108
1.5	12	24	24	36	36	36	36	204
1.6			36	48	48	48		180
1.7			12	12	12	12	12	60
1.8	6	6	24	24	24	24		108
1.9		6	6	24	36	36	36	144
1.10			24	24	18			66
2.1			24	36	36			96
2.2			12	24	24			60
3.1			12	12	12	12	12	60
3.2	12	12	12	12	12	12	12	84
3.3			12	12	12	12	12	60
4.1	24	48	48	48	24	12		204
4.2	12	30	48	48	24	12		174
4.3			36	48	24	12	12	132
4.4			12	36	24	12	12	96
4.5			12	36	24	12	12	96
4.6			12	36	24	12	12	96
4.7			12	36	24	12	12	96
4.8			12	12	12	12	12	60
4.9				12	12	12	12	48
5.1			12	12	36	36	36	132
6			6	6	6	6	6	30
Total	90	198	624	894	756	390	246	3198

Table 4-1. R&T Segment Summary of Required Staff Resources

Task	DGSA Transition Plan Schedule	S/M
	Research & Technology Segment Transition Schedule	3064
1	Separation Technology	1590
1.1	Separation Kernel Development	624
1.1.1	Security Policy Enforcement Function (SPEF)	96
1.1.2	Security Policy Decision Function (SPDF)	96
1.1.3	Security Policy Rules Representation	144
1.1.4	Information Domain Policies and Rules Prototypes	96
1.1.5	Tools for Security Policy Rules Production	96
1.1.6	Standard Kernel Interface	96
1.2	Security Contexts	48
1.3	Security Associations	48
1.4	Other Security Critical Functions	108
1.5	Formal Methods for Separation Kernel Evaluation	204
1.6	Real-Time Distributed Kernel Operations	180
1.7	Separation Kernel Software Evaluations	60
1.8	Object-Oriented Technology Prototypes	108
1.9	Sponsored Product Developments	144
1.10	Alternative Separation Technologies	66
2	Security Management Information Base	156
2.1	SMIB Maintenance	96
2.2	SMAP/SMIB Interface	60
3	Key Management Infrastructure	204
3.1	Information Domain/EKMS Relation Modeling	60
3.2	Key Management Protocol Standards	84
3.3	Key Management Infrastructure Standards	60
4	Security Mechanisms	1002
4.1	Programmable Cryptography	204
4.2	Software Cryptography	174
4.3	Fault Detection, Correction, Tolerance for Security	132
4.4	Tamper Proofing	96
4.5	New Tempest Requirements and Mechanisms	96
4.6	Security Mechanism Metrics	96
4.7	Security Mechanism Catalogs	96
4.8	Threat Analysis Tools	60
4.9	Vulnerability Analysis Tools	48



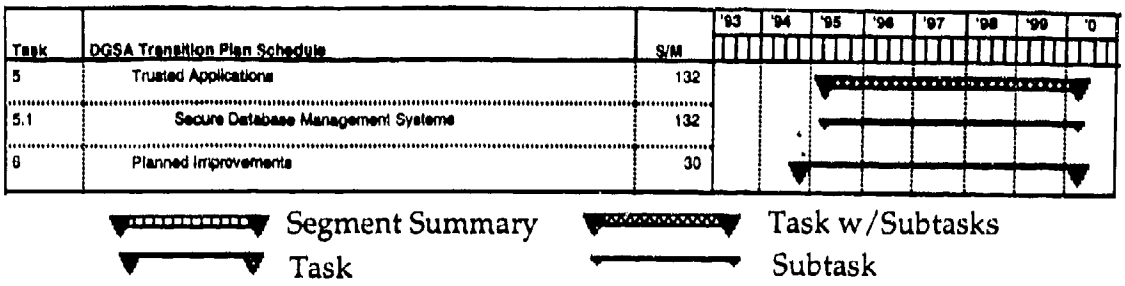


Figure 4-1 Research and Technology Segment Transition Schedule

4.4.8 Segment Status

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

Subtask 1.1.1 Security Policy Enforcement Function (SPEF)

This difficult part of the Research and Development (R&D) has been progressing satisfactorily. A prototype will be available by summer 1995 that will demonstrate at least portions of the SPEF and SPDF. Although full network services will not yet be present, several of the servers will be demonstrated including the authentication and cryptographic server. The system will be initially tested without invoking specific security policies. These tests will indicate points of weakness in the design, and will form the beginning for baseline measurements of the penalties for invoking cryptographic services.

Subtask 1.1.2 Security Policy Decision Function (SPDF)

The status on this subtask is identical to Subtask 1.1.1.

Subtask 1.3 Security Associations

The strategy embodied in this subtask is to use the Key Management Protocol of the IEEE 802.10 LAN-MAN standard. R2 is active in writing this standard and has a current effort to introduce modifications to make it fit more closely with what is needed in the DGSA. Related efforts include presenting this protocol to the IETF by April 1995 for their use on Internet. Success in these activities will mark a significant milestone in the DGSA transition.

Subtask 1.4 Other Security Critical Functions

Many of these functions are covered under Subtask 1.1.1 above. Relevant research at Portland State University is developing an X-windows system in which flexible policies are addressed. The research is aimed at reducing the amount of code needed to establish, maintain, and control these policies. This may help reduce the quantity of trusted code necessary for security critical functions.

Subtask 1.5 Formal Methods for Separation Kernel Evaluation

While no results are yet available, formal method evaluation is part of a current R2 contract with SCC to furnish a microkernel-based operating system.

Subtask 1.6 Real-time Distributed Kernel Operations

This work is underway, based on T-MACH.

Subtask 1.8 Object-Oriented Technology Prototypes

The relationship of object oriented technology with microkernels is getting increased attention, and is under study by R2.

Subtask 2.1 SMIB Maintenance

The Multilevel Information System Security Initiative (MISSI) program is supporting SMIB development and may have application to DGSA.

Subtask 2.2 SMAP/SMIB Interface

The SMAP/SMIB development underway for the MISSI program may have application to DGSA.

Subtask 3.1 Information Domain/EKMS Relation Modeling

While there has been no specific progress on this task, R2 has produced studies on how to decentralize key management, a necessity when considering DGSA connectivity to the National Information Infrastructure(NII). Work on creating an infrastructure to support key management is being planned, and may be carried out by the General Services Administration (GSA). GSA is in the process of gathering Government agency requirements and may be able to begin the design of a hierarchical infrastructure by the end of 1995.

Subtask 3.2 Key Management Protocol Standards

IEEE-802.10 is the emerging key management standard, but has not been fully adopted by the national security community. Additions to the standard are needed to meet DoD criteria. Representatives from NSA are part of this standards activity and are proposing security relevant changes. The effort has been expanded to encourage the IETF to adopt the IEEE set of standards. This proposal is due to be submitted to IETF by April 1995.

Subtask 3.3 Key Management Infrastructure Standards

See progress under Subtask 3.1 above.

Subtask 4.1 Programmable Cryptography

With the advent of Fortezza, Capstone, and Clipper, only the assurance aspects of programmable cryptography remain to be researched. There is no further progress in developing assurance mechanisms to be reported at this time.

Subtask 4.2 Software Cryptography

NSA objects to software cryptography because anyone with access to the program can modify it. If used in an inadequately protected environment, the software cryptography is highly vulnerable. While there have been considerable efforts over the past few months, there is no significant progress to be reported on solving this significant problem.

Subtask 4.3 Fault Detection, Fault Correction, Fault Tolerance for Security

Faulty hardware or software must be detected and corrected without causing security compromises. Fault-tolerant deigns must include awareness of security impacts. Fault monitoring, as it pertains to security impacts, must be accomplished as part of security management. This subtask is showing some progress in the investigation of fault detection, correction, and tolerance in an effort to enhance the basis for secure end system operation. The progress to date has been in developing techniques, processes, and tools that will quantify the probability that, in the presence of faults, a system may deviate from specified correct functionality. R2 is sponsoring two research efforts to develop security fail-safe metrics, one at Motorola and one at Research Triangle Institute (RTI), Motorola has developed a metric called State Transition Chain Analysis (STCA) based on Markov models and, to some extent, reliability calculations. This process will be tested on the NSA KG-189 design to help evaluate the usefulness of this metric process. RTI has defined a set of fail-safe attributes related to circuit structure and has developed a set of measurements for these attributes. RTI will next develop an automated tool for measuring the overall security fail-safe attributes of a design and identifying the conditions that lead to insecurities for a particular design.

Subtask 4.4 Tamper Proofing

Tamper proofing is used to prevent an adversary from tampering with security-critical hardware in end system components. Progress to date has been made in proposing means of protecting the MISSI Personal Computer Memory Card International Association (PCMCIA) cards. In 1994, R2 began selecting several tamper technologies that show potential for protecting critical circuit components as well as PCMCIA devices. Three techniques are currently under development. These are: Phosphor Label, Spatially Distributed Key, and a third technology. Spatially Distributed Key consists of a passive key which is unique to each card, and is embedded in the PCMCIA Card and is difficult to reverse engineer. The third technology consists of developing a potting compound that is difficult to drill through, or remove, or replace.

Subtask 4.6 Security Mechanism Metrics

Metrics are needed to characterize the relative strengths of security mechanisms in support of the absolute protection prescribed by the DGSA. Such metrics will support judgments made about the adequacy of security mechanisms applied to end systems communicating to share information. An R2 program is being started to gather the results of state-of-the-art research already accomplished by Government, industry, and academia on measuring attributes associated with security. A three month effort is planned to consolidate the existing state-of-the-art techniques for fail-safe, fault detection, trusted software, tamper proofing, reverse engineering, etc. to the extent these exist. This work will be performed in parallel with a literature search and discussions with Government, industry, and academia researchers to determine other information sources. A report is the short-term output expected from this program, to begin in early 1995. Follow-on actions will be guided by the results in the report.

Subtask 4.7 Security Mechanism Catalogs

Support for the user is required to employ the particular security services required by the security policy. This subtask requires development of that support in the form of user-friendly catalogs that describe trade-offs of various security mechanisms. Initiation of this task is included in Subtask 4.6.

Segment Tasks Not Being Performed

Subtask 1.1.3 Security Policy Rules Representation

This work has not started.

Subtask 1.1.4 Information Domain Policies and Rules Representation

This work has not started.

Subtask 1.1.5 Tools for Security Policy Rules Production

This work has not started.

Subtask 1.1.6 Standard Kernel Interface

This work has not been started.

Subtask 1.2 Security Contexts

The work on this will begin in summer 1995 as part of Subtask 1.1.1.

Subtask 1.7 Separation Kernel Software Evaluations

This subtask requires the efforts of the NSA C organization. C is resource limited and their participation is invited, but not expected until DGSA is in a more advanced development stage. This work has not been started.

Subtask 1.9 Sponsored Product Developments

The research and development on SPDF and SPEF has advanced to the point where the technology can begin transition to commercial operating systems. So far, none of the major vendors have been interested in the cooperative or sponsored effort. Transition of this research needs help from the transition team to advertise a market or otherwise interest vendors in adopting security-oriented microkernels as part of their emerging operating systems development.

Subtask 1.10 Alternative Separation Technologies

No work has been started for this subtask.

Subtask 4.5 New Tempest Requirements and Mechanisms

No work has been started for this subtask.

Subtask 4.8 Threat Analysis Tools

No work has been started on this task.

Subtask 5.1 Secure Database Management Systems

This subtask requires identification of any remaining research efforts and to perform the work necessary to apply secure databases to the DGSA. There is no progress on this task.

Task 6 Planned Improvements

No work has been started on this task.

5. SECURITY MANAGEMENT SEGMENT TRANSITION STRATEGY

5.1 Introduction

There has long been a need for a standardized definition of the scope of Security Management (SM) and a useful model of SM. The definition needed includes the data structures, management applications, security manager roles and responsibilities, and communication and security protocols which support SM. There is also an evolving need to define a standardized security infrastructure which will support the needs of SM functions. New electronic key management systems and universal Identification and Authentication (I&A) structures and registrars are needed, perhaps in a single security infrastructure.

The SM segment provides a strategy for furthering the SM model presented in the DGSA and for establishing the infrastructures, standards, and protocols necessary to support that model.

The DGSA presents a model for SM which needs to be further developed and implemented. The DGSA model is founded on the concept that SM is the "glue" which binds security contexts to security associations. The DGSA defines the relationships of security contexts and security associations and describes how SM works in local and distributed modes of control. The model includes standard data structures (managed objects and attributes), communications and security protocols, and SM applications.

SM under the DGSA gives new flexibility to users of information systems to choose by whom, how well, and at what cost security will be provided. Users may choose which security services they desire and which are to be controlled locally or remotely. The services can be applied, if desired, to well-organized, large or small information domains each with its separate security policy. SM under the DGSA represents a departure from the single minded central authority approach to embrace the concepts of distributed and cooperative control. The DGSA responds with SM that fits the requirements for open systems and interoperability.

5.2 Background

The purpose of SM is to initialize, monitor, control, maintain, and coordinate the resources and activities pertinent to information security. SM ensures that the security policies of communities of interest are enforced and that information and information systems are protected. As a distributed functional entity, SM encompasses an infrastructure of support personnel, applications, information bases, and security infrastructure support systems (e.g., electronic key management systems, certificate authorities). SM in the DGSA deals with:

- The environment in managing doctrinal (physical, administrative, and personnel) mechanisms established to protect LSE resources;
- End systems and relay systems and the information domains which reside in them, in supporting the establishment, maintenance, and enforcement of implemented security policy and its operating realization through security contexts;
- The transfer system composed of the local communication systems and portions of the end systems and the relay systems, in supporting the establishment and enforcement of security associations utilized to bind near-to-far distributed security contexts; and,
- The commercial wide area communications network portion of the transfer system, in supporting the security service of availability.

SM is widely accepted in DoD and to a lesser degree in International Standards Organization (ISO) as part of the system management which is typically depicted as a hierarchical structure for control of "the network". Through this structure many types of information are gathered through monitors and are moved up the layers for analysis and decision. Decisions are propagated down through the layers in the form of controls. With this view of information systems, major efforts are underway to standardize what is to be monitored and in what format things will be reported. Similar standardization efforts deal with what needs to be controlled and what command formats are needed. The only systems which come close to this model are wholly owned and operated national or commercial communications systems. Information systems connected by these CNs are in dire need of system and SM. The Internet is without any perceptible structure for either communications or information systems management. In all cases there is no definition or working model for SM.

The concept of centrally managed, hierarchically controlled security in globally interconnected networks of information systems is impractical. Our traditional approach is to build private, closed networks and to build gateways to allow and control the flow of information between them. Frustrations with the cost and with the policies and authorities who control the many gateways needed soon give rise to the notions of "bypass the gateway security for operational necessity".

The DGSA places SM in the end system. It defines security contexts and security associations in and between end systems as the fundamental concepts for building any desired structure for the SM of an indefinite number of information systems. There can be many different , coexisting structures even supported within a single end system. SM is defined in the DGSA as being independent of system management with the assumption of cooperation for service and performance between security and system management.

5.3 Transition Approach

The full scope of the transition to DGSA SM is enormous as the tasks and resources will show. There are, however, some modest efforts which can put the DGSA model into implementation. The proof-of-concept tasks can provide real implementations for near-term use as the prototypes are developed. In the final analysis though, the segment initiates massive efforts on a global scale to achieve international interoperability.

The transition approach to security management includes analysis, concept of operation (CONOP) development, proof-of-concept development and demonstrations. In addition it will attempt to standardize major portions of the security management infrastructure and provide technology insertion assistance to products and the LSEs in transition. This segment will also support the revisions and maintenance of the DGSA document. Of particular importance in this approach are the following objectives which will be met in a combined effort with the Research and Technology Segment:

- Research of security policy parameters for both the SPDF/SPDF defined in the DGSA;
- Proof of concept demonstrations of SMAP, with interfaces to security critical functions;
- Development of supporting security infrastructures (e.g., electronic key management systems and universal I&A data structures, protocols, and registration systems);
- Standardization of the objects and attributes of the SMIB, and development and standardization of new SM models;

- Development of mechanism catalogs and security metrics which can be used consistently throughout the System Security Engineering Process;
- Development of new SM protocols where existing and evolving standards are not sufficient; and,
- Development of SM design guidelines to assist product vendors and SM software developers

5.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 5.4.16 Subsection 5.4.17 provides the status of each segment task.

5.4.1 Task 1: Revisions to the DGSA

Description: This task will staff the improvement of the DGSA document to react to comments, supply more worked examples, complete the appendices, and move from draft to first issue. The DGSA needs to be harmonized with (synthesized into) the TAFIM and placed into coordination.

Responsible Organization: Primary: DISA CISS A&E directorate, NSA V & X groups. Support: NIST.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy Task 1		N/A
Required Staffing:	18 staff months	1994	
	12 staff months	1995	
	6 staff months	1996	
	6 staff months	1997	
	6 staff months	1998	
Total	48 staff months		

5.4.2 Task 2: Research Security Policy Parameters for SPDF/SPEF

This task is composed of four subtasks involving proof of concept development and testing of the SPDF and SPEF to ensure that such a policy decision and enforcement mechanism is practical. This task will also ensure that the SPDF/SPEF can support multiple, simultaneous security policy instantiations. Development of the SPDF and SPEF is an R&T segment task. The sub tasks defined here are closely coupled and aligned with R&T tasks to develop the SPDF and SPEF and tool(s) necessary to insert and maintain those portions of the domain specific security policies which are handled by the SPDF/SPEF. This task requires development and assistance in the SPDF/SPEF insertion of security policy parameters. The basis of the task is to develop "machinable" rules and attributes which represent documented security policy (system

and domain), and then to code/implement the rules and attributes in the SPDF which are subsequently interpreted and placed in SPEF cache or tables. The subtasks require two iterations of implementation and testing to ensure an effective concept proof. Lessons learned and problems encountered in the first iteration are used to enhance and modify the implementation in the second iteration.

Subtask 2.1: Code/Implement SPDF/SPEF in Prototype Platforms

Description: This subtask requires use of an appropriate SPDF/SPEF implementation, if one exists from prior R&T activities. If an appropriate implementation does not exist from prior R&T activities, then software modules will be developed on a standard UNIX operating system to simulate these functions. If simulation is pursued the modules will be implemented in accordance with SPDF/SPEF specifications. This subtask is composed of two parallel efforts. The first will require coding and implementing the SPEF/SPDF functions (if necessary, based on timing), and the second will require developing a tool to implement security policy rules and attributes which can be interpreted by the SPDF. For example, this might be a tool developed using a compiler-compiler parser, like YACC.

Responsible Organization: Primary: NSA R2. Support: CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Subtask 1.2
Required Staffing:	54 staff months	1995		

Subtask 2.2: Test Suitability of Policy Tools

Description: This subtask requires testing and enhancements made to the SPEF/SPDF implementation in the prototype. This task includes analysis and decisions on how to proceed based on the results of the testing. Of primary interest in this testing task is the ability to translate written domain security policies into executable rules and mechanism calls when translated from the SPDF to the SPEF. Testing will also ensure the ability exists to alter security policy for any particular domain and to add new domain security policies to the implementation.

Responsible Organization: Primary: NSA R2. Support: CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1, Subtasks 5.1, 5.2	STD	Subtasks 3.1,3.2
Required Staffing:	30 staff months	1995		

Subtask 2.3: Revise the Security Policy Parameters

Description: This subtask allocates resources for modification deemed necessary as a result of the first iteration of development and testing, and enhances the tool to make it user friendly, for example, a graphical user interface (GUI) with icons will be added to make the tool more user friendly and appealing for demonstration.

Responsible Organization: Primary: NSA R2l. Support: CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	N/A	
Required Staffing:	66 staff months	1996		

Subtask 2.4: Retest Policy Tools

Description: This subtask requires making any minor adjustments and re-testing for the SPEF/SPDF implementation in the prototype. This last subtask includes demonstrating the deliverable from the prototyping task to various organizations and industry representations interested in the results of the subtask. The conclusion of this subtask also includes a report describing all aspects of the effort and the technical results of the testing activities.

Responsible Organization: Primary: NSA R2. Support: CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	STD	Subtasks 3.1,3.2
Required Staffing:	36 staff months	1996		

5.4.3 Task 3: Develop Prototypes for Proof of Concept

Description: This task requires development of platforms for the testing and proof of concept of DGSA Security Management concepts. The task includes support to policy preparation, information domain management, system management, and the development and testing of new protocols. These activities will be coordinated and correlated with R2 activities, and, where appropriate, be provided to R&T prototyping activities and/or given to industry for technology insertion.

Responsible Organization: CISS A&E Directorate, NSA X, R2.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Subtask 1.2
Required Staffing:	30 staff months	1995		
	66 staff months	1996		
	78 staff months	1997		
	48 staff months	1998		
Total	222 staff months			

5.4.4 Task 4: Development of SMAP

Description: This task requires specification and development of the software application which will support security policy building, installation, and maintenance. The SMAP development is intended as a major tool to be used by security administrators. Work on this effort in FY94 and 95 will be directly affiliated with the task 3 prototyping efforts. Work on this effort in FY96 and 97 will be directly affiliated with technology insertion activities with industry, on going internal NSA product development programs, and R&T separation technology prototypes.

Responsible Organization: CISS A&E Directorate, NSA R2.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Subtask 1.2
			STD	Subtasks 3.3,4.1
Required Staffing:	15 staff months	1995		
	15 staff months	1996		
	6 staff months	1997		
Total	36 staff months			

5.4.5 Task 5: Development of Supporting Security Infrastructures

Description: This task will require a set of major programs to develop or modify existing Security Infrastructure systems for the provision of identification and authentication, digital signatures, authorization certification, general notarization, key management, and non-repudiation services. (Includes activities such as a new EKMS, DSS, benign fill, downloadable algorithms, etc.) Task 5 includes a new EKMS to deal with contemporary key management problems that can not be accommodated with the current EKMS. The new system will be based on standards, provide flexibility for growth, and will allow integration of the current/evolving EKMS if the decision is made to do so. This task also includes a great deal of the Infrastructure 2000 work being recommended. Without the new EKMS focus, the staff hours projected decrease from 224 staff years to about 40 staff years for Task 5. Where possible this task will build on the work being performance to support the MISSI products and the DMS program.

Responsible Organization: Primary: NSA V4. Support: NSA X1, R2, CISS A&E.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	STD	Task 2, Subtasks 3.3,4.1,4.3
Required Staffing:	252 staff months	1995		
	384 staff months	1996		
	912 staff months	1997		
	1140 staff months	1998		
Total	2688 staff months			

5.4.6 Task 6: Research and Standardization of SMIB Objects & Attributes

Description: The SMIB contains the reference and control information which enables Security Administrators to manipulate security critical resources. In conjunction with Task 2, policy and other elements of the SMIB will be defined and standardized where possible. The SMIB will make use of existing standardized security attributes (e.g. from EKMS, international standards, and where applicable, from MISSI Network Security Management (NSM) component specifications). Results from this task are used directly by Task 3.

Responsible Organization: Primary: CISS A&E Directorate. Support: NSA R2, X1.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	STD	Subtasks 3.1,4.2,4.3
Required Staffing:	30 staff months	1995		
	42 staff months	1996		
Total	72 staff months			

5.4.7 Task 7: Review & Planning Transition Enhancements for NSM Products

Description: This task will track ongoing NSM products development work and advise on transition enhancements that should be made to Local Authority Workstations (LAWs), Audit Manager, Secure Network Server (SNS), and other NSM products. The purpose of the task is to ensure NSM products are implementing appropriate standards and proven concepts of security management on a timely basis, and to ensure NSM product design does not arbitrarily shut out such enhancement potential. This task also requires advising on the integration of the DMS program concepts and products with the NSM Products.

Responsible Organization: Primary: DISA. Support: CISS A&E Directorate, NSA R2, J03, X1.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy Task 1		N/A
Required Staffing:	36 staff months	1995	
	48 staff months	1996	
	48 staff months	1997	
	36 staff months	1998	
Total	168 staff months		

5.4.8 Task 8: Development of Mechanisms Catalog and Security Metrics

Description: This task will develop the format and content of a catalog of security mechanisms. Security mechanisms implemented in security products will be cataloged along with a system of metrics and mechanism interdependencies, interoperability profile, and proper (potentially improper) ways to configure, initialize and use each of the mechanisms. The metrics will be used to define the type, doctrine, and strength of mechanisms. The cataloging process will employ a methodology for interdependence analysis. This effort is closely affiliated with component/product security profiling. The mechanism catalog which evolves will be maintained by the CISS Products directorate and/or the NSA Profiling organization(s) and be integrated with the Products Database that will be developed by the Products Segment.

Responsible Organization: Primary: CISS A&E. Support: NSA X1, NSA Profiling Organizations, CISS EC&A, and NSA Evaluation Organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Subtask 1.2
	C&A	Task 5	C&A	Subtask 3.3
			STD	Subtasks 4.3,4.4, 5.1, 5.2
			CN	Subtask 4.3
Required Staffing:	36 staff months		1995	
	48 staff months		1996	
	48 staff months		1997	
	36 staff months		1998	
Total	168 staff months			

5.4.9 Task 9: Development of Security Management Model

Description: This task requires development of a security management model that will be significant to the understanding, standardization, and implementation of security management in real open systems. The model will illustrate, and serve in evaluating, the relationships of users, applications, security service provisions, and security administration in local and distributed management arrangements. It will significantly enhance the simple Manager/Agent model, which is all that exists in standardization bodies today.

Responsible Organization: Primary: CISS A&E Directorate. Support: NSA R2 and X1.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Subtasks 3.1,7.1,7.2
			STD	Subtask 4.3
			LSE	Task 6

Required Staffing: 12 staff months 1995

5.4.10 Task 10: Develop Security Management Protocols and Standards

Description: This task requires the continuation of the development of standard security management protocols and general security management standards, working in standards organizations such as the IEEE 802 Standard for Interoperable LAN/MAN Security (SILS) committee and ISO SC21 and SC6 committees. The results of these already established activities are expected in FY95 and to impact product requirements beginning in FY96.

Responsible Organization: Primary: CISS A&E Directorate. Support: NSA R2, NIST, and DISA CFS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	CN	Subtask 4.3
			STD	Subtask 4.3

Required Staffing:		
	96 staff months	1995
	60 staff months	1996
Total	156 staff months	

5.4.11 Task 11: Security Awareness and Administrative Training

Description: This task requires developing and supplying the raw materials to the CISS Professionalization Directorate for creation and teaching of security administrator training. The effort continues throughout standards, protocols, and guidelines development.

Responsible Organization: Primary: CISS A&E Directorate, CISS Professionalization Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Task 5

Required Staffing:		
	12 staff months	1995
	12 staff months	1996
	12 staff months	1997
	12 staff months	1998
Total	48 staff months	

5.4.12 Task 12: Develop Security Management Design Guidelines

Description: This task will produce the guideline documents that can be used by system engineers to design their specific security management architecture. These documents will address local and distributed management, and the choices for allocating management responsibilities to users, system administrators, or information domain administrators. Iterative guideline documents will be released in FY95, FY96, and FY97, with final guideline releases in FY98.

Responsible Organization: Primary: CISS A&E Directorate. Support: NSA X1, V4 and the NSA profiling organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1, Subtask 5.3	Prod	Subtask 1.2
	C&A	Subtask 3.3, Task 5	CN	Subtask 4.2
			E&T	Task 5
			STD	Subtask 4.3

Required Staffing:	42 staff months	1995
	24 staff months	1996
	24 staff months	1997
	24 staff months	1998
Total	162 staff months	

5.4.13 Task 13: Define Interactions with Users and Security Managers

Description: In conjunction with Tasks 4 and 8, the functions and processes to be supported for users and security administrators need to be defined and then tested through development of a proof of concept prototype. This task will define the interactions SM functions must support for normal users and security managers.

Responsible Organization: Primary: CISS A&E Directorate. Support: NSA X1, V4, R2, and the NSA profiling organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	CN	Subtask 4.2
	C&A	Subtask 3.3, Task 5	E&T	Subtasks 4.2,7.1, 7.2
			LSE	Task 6

Required Staffing:	18 staff months	1995

5.4.14 Task 14: Perform Security Management Technology Insertion

Description: Under this task, guidance and proven security management technology insertion into on-going security product development programs will be provided. All major development programs (e.g., Global Grid (GG), DISN, Defense Message System (DMS), MISSI) will collectively influence the definition and development of SM. In return, the segment defined security management must be inserted into all programs through the preparation of design documentation and assistance in its preparation.

Responsible Organization: DISA CISS A&E Directorate, NSA R2.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Subtask 1.2

Required Staffing:	39 staff months	1995
	27 staff months	1996
Total	66 staff months	

5.4.15 Task 15: Support Other Segments with Planning Assistance

Description: The SM segment shares information and task responsibilities with all of the other segments. There are significant overlaps in task definitions between segments which demand joint planning to accomplish transition to the DGSA. This task is a place holder for SM assistance to other segment task areas for planning and coordination over the next year.

Responsible Organization: CISS A&E Directorate, DOTS Core Team.

Inter-task Dependencies:	Input Dependencies Policy Task 1	Output Dependencies N/A
Required Staffing:	18 staff months 1995	

5.4.16 Resource Summary and Transition Schedule

Table 5-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 5-1 shows the segment transition schedule.

	Resources Required in Staff Months					
Task	FY94	FY95	FY96	FY97	FY98	Total
1	18	12	6	6	6	48
2.1		54				54
2.2		30				30
2.3			66			66
2.4			36			36
3		30	66	78	48	222
4		15	15	6		36
5		252	384	912	1140	2688
6		30	42			72
7		36	48	48	36	168
8		36	48	48	36	168
9		12				12
10		96	60			156
11		12	12	12	12	48
12		42	24	24	24	114
13		18				18
14		39	27			66
15		18				18
Total	18	732	834	1134	1302	4020

Table 5-1. SM Segment Summary of Required Staff Resources

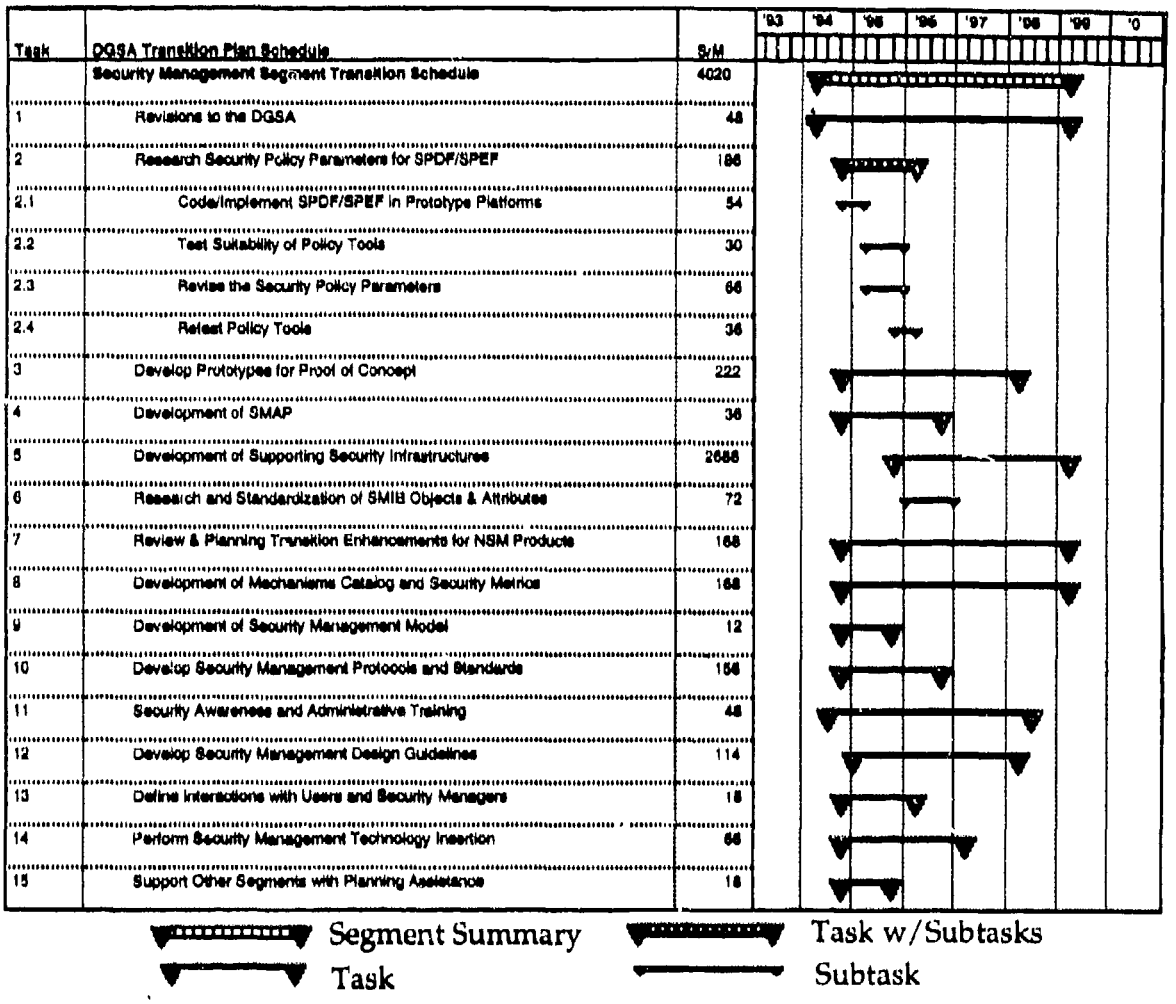


Figure 5-1 Security Management Segment Transition Schedule

5.4.17 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

None of the segment tasks are being executed.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1, 2.1, 2.2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

(This page is intentionally blank.)

6. COMMUNICATIONS NETWORKS SEGMENT TRANSITION STRATEGY

6.1 Introduction

The DGSA analysis of DoD requirements for inter-site communications leads to a markedly different approach to communications network (CN) security than that which has been followed over the last several decades. From the DISSP.SP1 and general DoD requirements for computer communications presented in the TAFIM, several principles are stated and conclusions drawn. For example, to satisfy DoD mission requirements (such as increased global communications connectivity) in an economically feasible way, LSEs and CNs must implement international or national standard protocols. In addition, common carrier CN service should be employed unless there are overriding TFS requirements, and LSEs must take almost complete responsibility for implementing security services that are responsive to the security requirements of specific missions, expecting only assured service (availability) from the CN. The CN transition strategy and specific tasks presented in Section 6.4 respond directly to these principles.

The CN segment team is composed of personnel from the DISO Data Services Division, Joint Interoperability and Engineering Organization (JIEO) Center for Engineering, NSA, and the MILDEPs. The CN segment works closely with the LSE Segment, often appearing as a single combined working group. The segment lead for CN is a representative of the DISA Enterprise Integration and the CFA.

The current and foreseeable trends in cost-saving efforts within the Government, especially DoD, will be greatly aided by the DGSA's recommendation to reduce Government-owned or operated CNs. By requiring the use of standard communications protocols, interoperability will be improved in line with stated DoD requirements. The most far-reaching DGSA impact on CNs is implementing security services in LSEs. This will allow the eventual removal of devices that implement security services for large groups of end systems, such as firewalls, and switch and router encryption systems. These devices make true interoperability difficult, if not impossible, to achieve and they are not able to provide security services appropriate to a wide variety of security requirements. In addition, such devices are often expensive to procure and maintain. LSEs will be able to provide security services that are appropriate to specific mission requirements. The DGSA approach to TFS will also result in cost reductions and improvements in interoperability by providing a metric to establish the exact TFS requirements for organizations. Additionally, organizations will be better able to take advantage of leading edge services as common carriers make them available, rather than waiting to be able to afford those improvements through acquisitions.

6.2 Background

There are a large number of DoD owned and operated CNs under the control of various services and agencies. Although there are some existing plans for upgrading or moving some of these CNs to common carrier resources (e.g., Defense Information Infrastructure (DII), Post-FTS 2000), there is not a coordinated effort to carry out the kind of transition implied by the DGSA. Some of the direction on which information systems will continue in the long term, expected as a result of the DISA CFII decisions, will help resolve CN planning in some cases. The lack of a comprehensive TFS policy gives many organizations an excuse to avoid the planning that would bring their CNs into line with DGSA concepts.

Some of the specific tasks called out in Section 6.4 are already in progress. Recent architectural activities for DoD (e.g., DII Target Security Architecture) and other Government

network planning (e.g., Post-FTS 2000) have taken DGSA principles into account and it is expected that more will do so in the future.

As noted earlier, the CN segment is critically dependent on progress in the area of LSE assumption of security service responsibility. To the extent that this progress is lacking, the CN transition goals will be delayed. There is a reluctance on the part of planners to extend their sights to a time which is somewhat indeterminate. That is, it is not possible today to offer a guaranteed date by which the CN transition goals can be met. A related problem is that there are still considerable resources being invested by vendors, researchers, and consumers in network component-based security solutions. Getting attention for a completely different paradigm is difficult.

6.3 Transition Approach

The CN segment interfaces with those organizations responsible for defining the DoD goal communications architecture in support of both strategic and tactical entities. Important contributions to the development of the DoD communications networks during the transition period will come from the technological developments produced by commercial organizations. The CN segment will, therefore, keep abreast of the latest technologies.

Several major programs are already underway that address the transition of DoD communication systems toward the future. The CN segment leverages off of these on-going activities and, if possible, steers these activities toward the DGSA requirements. On-going activities must be influenced to ensure that the DGSA requirements are being met. Although the ultimate goal of the DGSA is for CNs to provide only availability as a security service, utilization of security features of CNs until appropriately implemented LSEs are fielded will remain an important consideration. Thus, major trends and programs in the CN area need to be identified, as well as the major product contributors of both COTS and Government-off-the-shelf (GOTS) products. The CN segment will determine how involvement in on-going communications transition processes can be best pursued. The CN segment will also identify approaches that will ensure that the DGSA requirements are adequately satisfied during these transitions, as well as at completion of the transitions.

The strategy for the CN segment involves the following activities: 1) identifying the major DoD programs that will need to transition their CNs, 2) defining methods for influencing the transition strategies of these programs, 3) tracking the ongoing activities of these programs to ensure that they are able to achieve the DGSA targets, 4) identifying specific security needs during the transition periods.

The major aspect of CN transition, provision of the availability security service, is dependent on a chain of activities beginning in the R&T segment, and continuing into the Products and LSE segments. Only as end systems and LSEs are able to provide appropriate protection to mission functions can the CN be relieved of other security responsibilities. There will not be a single time when this will be achieved. For missions with less stringent protection requirements, the transition can occur sooner. Each organization will have to judge when the appropriate LSE security technologies are available to satisfy its needs.

Some tasks in Section 6.4 are scheduled relatively soon to provide the basis for the other major CN segment transition elements. The TFS policy and subsequent identification of existing missions requiring long-term TFS protection can be expected by the end of CY95. The definition of availability criteria that form the contractual basis for subscribers to obtain service from common carriers will be completed during CY95. The remaining tasks will provide the potential for all non-TFS subscribers to be on public carrier networks by the end of CY2000. If

there are carrier capacity constraints or if organizations are not able to acquire the appropriate LSE components, the realization of this goal will be delayed.

6.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to initiate these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 6.4.5. Subsection 6.4.6 provides the status of each segment task.

6.4.1 Task 1: Define and Specify Availability Criteria

The purpose of this task is to create a means for subscriber organizations to accurately and unambiguously convey their availability requirements to common carriers. The ability to express availability requirements to common carriers (in a way that is more useful than the traditional percentage of time the service must be active) will become critical as the Government, and particularly DoD, moves away from owned or leased communications networks and toward bandwidth on demand services. Availability criteria for specification and for performance measurement need to be developed so that they can be conveyed unambiguously to carriers, including penalty clauses for not fully meeting the contracted availability requirement. The three subtasks of this task define the availability criteria, develop procurement specification techniques, and obtain consensus between DoD and the carriers.

Subtask 1.1: Define Availability Criteria

Description: Under this subtask, a set of parameters will be determined to accurately define and state subscriber availability requirements. The parameter definitions must be comprehensible to subscribers, usable by carriers, and available by source selection authorities.

Responsible Organization: Primary: DISA CFA. Support: DISA CISS A&E

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Task 9
			E&T	Subtask 3.1, Task 12

Required Staffing: 18 staff months 1995

Subtask 1.2: Create Techniques for Procurement Specification

Description: This subtask requires the development of techniques for specifying availability criteria in forms that will be contractually binding. Such techniques will be made available for use by subscribers in request for proposals (RFPs) or by carriers to describe offered services.

Responsible Organization: Primary: DISA CFA. Support: DISA CISS A&E

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Subtask 3.1, Task 12

Required Staffing: 6 staff months 1995

Subtask 1.3: Achieve Consensus of DoD and Carriers

Description: Agreement among subscribers and carriers that the results of Subtasks 1.1 and 1.2 are mutually acceptable is critical to the success of Task 1. This subtask will seek to achieve such consensus and provide feedback to Subtasks 1.1 and 1.2. In preparation for this task, the post-FTS 2000/DISN follow-on market survey and inputs from industry will be reviewed.

Responsible Organization: Primary: DISA CFA. Support: DISA CISS A&E

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Subtask 3.1, Task 12

Required Staffing: 12 staff months 1995

6.4.2 Task 2: Carrier Technology Insertion Support

Description: Various technologies may be used by common carriers to achieve a specified availability of service. When DoD has information or technology deemed useful to carriers or when carriers seek help in improving their availability service, DoD will support the carriers. Thus, efforts under this task are activated only on a supply and demand basis. This task is expected to be an ongoing activity into the long term. Example technologies include techniques for protection of management traffic, protection of physical assets, and alternate routing in stress situations. This work will build on the prior efforts of the NETS program and the ongoing activity of the GETS program.

Responsible Organization: DISA CISS, NSA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Subtask 3.1, Task 12

Required Staffing: Only the current allocation of resources to support the DISN-NT Acquisition is reflected here. For this specific application, resources have been assigned for 1995 and 1996: 6 staff months over the period 1QCY95 through 4QCY96.

6.4.3 Task 3: Traffic Flow Security

Under this task, a TFS policy will be created and recommended for the DoD. The Policy segment will complete the development of a DoD-wide TFS policy. The first subtask of Task 3 requires development and distribution of a TFS white paper which provides guidance for judging which subscribers have true TFS requirements. The second subtask proposes a TFS policy for DoD.

Subtask 3.1: TFS White Paper

Description: Under this subtask, a white paper was prepared that provides guidance for determining when true TFS mission requirements exist. The white paper existed in draft at the time this strategy was prepared, but required additional review. The results of this subtask will be forwarded to the Policy segment for coordination and approval as official DoD guidance.

Responsible Organization: NSA

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Policy	Task 3
			LSE	Tasks 4,8
			E&T	Subtask 3.1, Task 12
Required Staffing:	1 staff month	1994		
	3 staff months	1995		
Total	4 staff months			

Subtask 3.2: TFS Policy Recommendation

Description: The purpose of this subtask is to prepare a proposed DoD TFS policy. The proposed policy will be input to the Policy segment TFS Policy Development task.

Responsible Organization: NSA

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Tasks 1,3	LSE	Task 9
			E&T	Subtask 3.1, Task 12
Required Staffing:	10 staff months	1994		

6.4.4 Task 4: Baselines for CN Planning

Identification of current DoD-controlled CN assets (owned or leased) is required under this task. In addition, this task requires preparation of a plan for transitioning such assets to fee-for-service common carrier CNs. The three subtasks of this activity call for definition of the current baseline, development of guidance for migration, and preparation of an implementation plan.

Subtask 4.1: Baseline Definitions

Description: Under this subtask, information on all current and planned CN assets will be gathered. CN assets will include both TFS-protected and non-TFS-protected assets.

Responsible Organization: Primary: DISA. Support: CFA, CFII, and the CISS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Tasks 3,7
			E&T	Subtask 3.1, Task 12
Required Staffing:	120 staff months	1994		
	6 staff months	1995		
Total	126 staff months			

Subtask 4.2: Migration Guidance

Description: This subtask requires evaluations of the assets identified in Subtask 4.1. The assets will be evaluated for their suitability for current and planned mission uses and to determine how long the assets can economically be operated. The determination of asset suitability must be made separately for the TFS-protected and non-TFS-protected CNs. Possible evaluation categories for CN assets are: 1) replace as soon as possible (not able to meet mission needs, not economical to operate, not possible to upgrade); 2) need to replace soon but stopgap measures are available; 3) need to make significant fixes, but will be allowed to continue for a longer

period; and 4) continue operation as-is or with minor fixes until all other assets are converted to common carrier operation. The evaluation of assets will support a phased migration to non-TFS-protected common carrier CNs as budgets and related schedules allow. Similarly, the evaluations will guide the upgrade or replacement of the remaining TFS-protected CNs.

Responsible Organization: Primary: DISA. Support: CFA, CFII, and the CISS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Task 3
	SM	Tasks 11,12	E&T	Subtask 3.1, Task 12
	C&A	Subtasks 3.1,3.2		

Required Staffing:		
	40 staff months	1995
	60 staff months	1996
	20 staff months	1997
Total	120 staff months	

Subtask 4.3: Implementation Plan

Description: This subtask requires the results of Subtask 4.2 and knowledge of existing and planned interoperability products (i.e., gateways). Using this information, a plan for the migration of current subscribers to an appropriate CN resource, either TFS protected or non-TFS protected, will be produced. The implementation plan will be a set of architectural solutions for ensuring interoperability over the complete period of transition to the DGSA. Inputs will be required from the LSE segment to appropriately address interoperability issues.

Responsible Organization: Primary: DISA. Support: CFA, CFII, and the CISS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	E&T	Subtask 3.1, Task 12
	Prod	Task 2, Subtask 1.2		
	SM	Tasks 7,9		

Required Staffing:		
	40 staff months	1995
	60 staff months	1996
	44 staff months	1997
Total	144 staff months	

6.4.5 Resource Summary and Transition Schedule

Table 6-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 6-1 shows the segment transition schedule.

	Resources Required in Staff Months				
Task	1994	1995	1996	1997	Total
1.1	9	9			18
1.2		6			6
1.3		12			12
2		3	3		6
3.1	1	3			4
3.2	10				10
4.1	120	6			126
4.2		40	60	20	120
4.3		40	60	44	144
Total	140	119	123	64	446

Table 6-1. CN Segment Summary of Required Staff Resources

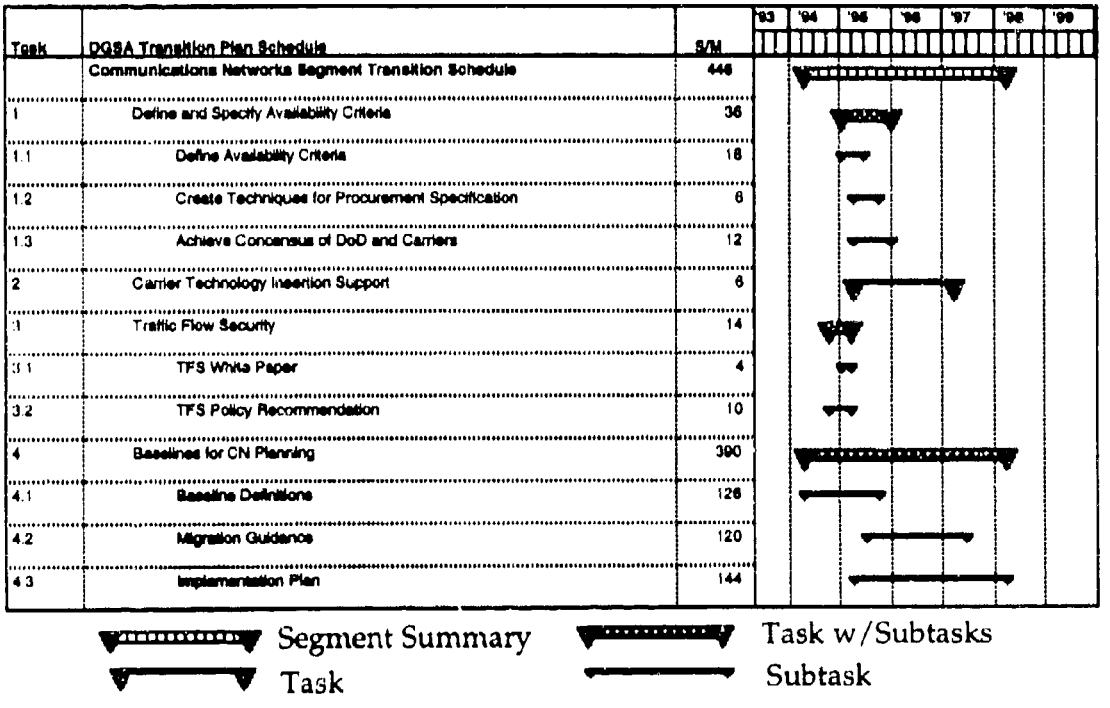


Figure 6-1 Communication Networks Segment Transition Schedule

6.4.6 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

Task 3.1 TFS White Paper

The white paper is under final review before being released in a draft version.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1.1, 1.2, 1.3. 2, 3.2, 3.3, 4.1, 4.2, and 4.3 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

7. PRODUCTS SEGMENT TRANSITION STRATEGY

7.1 Introduction

The Products Segment transition strategy addresses the concerns regarding the acquisition of efficient, affordable, interoperable, and relevant INFOSEC products that can be flexibly employed to meet the protection needs of operational systems. This transition strategy: (1) describes the Products Segment and its relation to the DGSA, (2) provides background information on INFOSEC products, (3) provides a transition approach, and (4) identifies specific tasks needed for transition.

The Products Segment conducts activities to promote the availability and awareness of COTS and GOTS INFOSEC products that will provide cost-effective, common component solutions for use in implementing DGSA-consistent system architectures. An example of this is the work being performed on the MISSI Program to develop firewalls and integrated identification and authentication mechanisms for the near-term. The products segment team leader is a representative from the CISS Products Directorate. The segment team membership includes representatives from the NSA Network Security Group (X Group) including the MISSI, the NSA (C71) Trusted Product Evaluation Program (TPEP), the military Services, NIST's Computer Systems Laboratory (CSL), and the CISS Multi-Level Security Program. Participation by other organizational representatives will be evaluated on an ongoing basis.

The Products Segment has three principal objectives: (1) improve the INFOSEC posture of the installed DoD information technology infrastructure, (2) improve the availability of INFOSEC products to support program transition to the DGSA, and (3) increase the awareness of current and future INFOSEC product suitability, availability, usability, affordability, and associated trends. The roles and responsibilities associated with the transition of INFOSEC products are outlined in Table 7-1.

7.2 Background

Most of the technology to be incorporated in DGSA-consistent products will come from R&T that is only now beginning. Thus, there will be few products in the current to near-time inventory to support transition to the DGSA. The imposition of standards will lag the technology development and further exacerbate the availability of interoperable, DGSA-consistent products. Critical system acquisition programs at this juncture include DISN/DISN-NT, DMS, Enterprise Information Systems Migration, and Global Command and Control System (GCCS). Since many of these programs are core infrastructure programs of the DII and since there are few DGSA-consistent products now available, these programs will need close review for future system upgrade phasing opportunities. These opportunities will require that system reengineering and/or reacquisition initiatives be taken to incorporate more DGSA-consistent COTS products or product features to strengthen security and improve integration and interoperability. Evolutionary experimentation with various products in highly visible prototype and advanced technology demonstration projects could improve the success of DGSA-consistent product and system transitions. The critical issue to be addressed through this process is rapid, cost-effective INFOSEC technology transfer into COTS products.

Responsibility	Participants
Characterize the INFOSEC product environment for system security components over specified periods of time.	CISS Products, NSA V Group, NSA X1, NSA C71, NIST, National Computer Security Association's National INFOSEC Exchange (NIE)
Perform detailed INFOSEC product assessments.	NSA C71 TPEP, NSA X1 Product Profilers; Navy, Air Force, NIST, Integrators, CISS Products, CISS EC&A
Coordinate the acquisition, storage, and retrieval of detailed INFOSEC product assessment information.	CISS Products, NIE
Provide detailed INFOSEC product assessment information, as part of the systems security engineering process, to system architects, lead security officers, and other designated members of a systems program management team.	CISS Products, NIE, all assessment participants
Maintain a continuous awareness of technology trends that are being manifested through research, technology transfer, standards development, product evolution, product market share, and DoD product acquisitions and inventories.	CISS Products, NSA R2, NSA V Group, NSA X1, NSA C71, NIST
Participate in the development and/or vetting of protection profiles expressing users' INFOSEC product requirements in terms of protection functions and assurances to accommodate the users' security policies and meet their risk-mediation strategies.	CISS Products, NSA C71, NSA X1, X2, and X3, , NIST
Provide accessibility for the vendor community to the DoD's repository of protection profiles that will guide the development of security functionality within an INFOSEC product.	CISS Products, NIST
Provide accessibility for system architects and system integrators to the DoD's repository of INFOSEC product profiles for use in crafting security architectural solutions as part of the systems security engineering process.	CISS Products, NSA X1 Product Profilers
Promote and facilitate the sharing of INFOSEC product technology between Government and industry.	CISS Products, NSA R2, ARPA, NIST
Provide industry with DoD perspectives to add focus to industry IR&D.	CISS Products, NSA R2, Services, ARPA
Facilitate the acquisition of INFOSEC products through common procurement instruments.	CISS Products, CISS MLS, CISS IP3, GSA
Coordinate the acquisition, storage, maintenance, and retrieval of information on DoD's INFOSEC-product installed inventory.	CISS Products, CISS EC&A, Military Services & Defense Agencies

Table 7-1 Roles and Responsibilities

The current state of INFOSEC products in progressing towards the DGSA-consistent systems is austere. There are few products that can support strict isolation and of those few, none are efficient and easy to use. Initial MISSI products and a limited set of TCSEC evaluated products at level B1 or above (e.g., compartmented mode workstations (CMWs), guards, and trusted operating systems, networks, and database management systems (DBMSs)) are the products that are available to implement systems security today. Looking forward over the next three years to the end of FY97, the outlook becomes only slightly more promising. System integration programs that were underway before or as DOTS began its implementation will primarily have products with older technology still in use. Initial MISSI technology developments will start to mature and product implementations will be incrementally improving.

The DMS program and perhaps some other system programs will begin implementing systems using selected subsets of available and procurable MISSI products. Acquisition program initiatives starting later in the period will be able to take advantage of any early progress made in DGSA-consistent product availability. These later starting programs will provide a greater opportunity to field newly developed DGSA-consistent technologies in COTS and GOTS products. Enhancing opportunities to employ new products, selectively incorporated into the FY98 to FY03 POM cycle, will be ready to be applied towards eliminating older computing, communications, and INFOSEC product technologies as FY97 closes out.

Among the most promising and perhaps the most needed technology to strengthen existing system protection is the security management and infrastructure support being provided by MISSI and the MISSI-using programs. The implementation strategy is to have no single central program responsible for implementing MISSI technology in DoD. Rather, the initiative relies on major joint programs and initiatives to implement the infrastructure and major system services, and to ensure interoperability and certified secure operations. NSA will provide centralized acquisition management for the initial procurement of most MISSI products with DMS managing the procurement of some of the remaining products and the rest provided through separately managed service/agency procurements from various vendors. The plan is that eventually all MISSI products will be acquired from a limited set of vendors using commodity buys and/or major system acquisition program contracts as the procurement instruments. NSA serves as the MISSI technology program manager. DISA CISS serves as the DII implementation support conduit between MISSI and major acquisition programs and initiatives. Throughout the systems security engineering lifecycle, Designated Approving Authorities (DAAs) retain their roles for operational risk acceptance in systems employing MISSI products.

MISSI products could provide a major first step toward widespread DGSA-consistent systems. There is a plan to evolve MISSI-based capabilities through an incremental MISSI technology update and periodic release configuration release schedule. Generic security architectures serve as the requirements for MISSI products-based security solution sets. The generic security architectures reflect common mission areas within the DoD. The security solution sets serve two purposes. First, they provide guidance for system security architects on the applicability of MISSI products and second they highlight unfulfilled requirements which will influence the development cycle. MISSI products will start to become available in FY95.

What is critical to widespread use is to match up the MISSI technology availability with product acquisitions. This may become problematic for the widespread implementation within DoD as a clear understanding of the scope and size of DoD needs for MISSI products has yet to be developed. Thus, while technology availability may occur in the near-term, it must be recognized that the current MISSI program, now supporting DMS, will not provide the necessary momentum to gain rapid and pervasive DoD use in the near-term. Demand from non-DMS programs is increasing, but MISSI's widespread availability may also remain questionable for the mid-term. There remains a significant, unplanned funding need to support DMS through FY02. Planning for the FY97-FY02 POM has begun and it is anticipated that much of the needed MISSI funding will be included in the POM submission as part of the Information System Security Program (ISSP). The funding strategy reflected in the MISSI implementation plan [9] relates overall MISSI funding needs to officially support requirements of DMS, but the plan also points out the need to include suggested financial planning wedges for funding non-DMS applications. This planning action may improve the outlook for the mid-term. It is the intent of the products segment to provide the most current information possible to program managers and system acquisition personnel to serve as critical inputs to Acquisition and Integration Strategies as well as Integrated Logistics Systems (ILS) plans.

The highest expectation for DGSA-oriented results from the R&T segment's research is separation kernels. The most important breakthrough that must occur in this research is

performance efficiency while achieving security effectiveness. The transfer of this technology must also be cost-efficient if it is to be incorporated into an increasingly competitive computer product market. These kernels will not be ready for widespread commercial production for several years (see R&T separation kernels). During this time, the initial separation kernel prototypes will be completed and new prototypes will be identified and initiated. Some modest efforts at commercial offerings may be evident.

The development of a standardized SAMP within the IEEE 802.10 standards community will enable faster realization of the protocol in commercial products. Products incorporating this protocol will provide the critical component for enabling protection of information domains in the context of distributed systems. A greater understanding of information domains will have been achieved. The elements of efficient security management will have undergone a few years of research and prototypes to support information domains will be in existence. The issues associated with security labels will have been studied and recommended standards will be either nearing completion or will be well along toward completion. It is anticipated that these particular standards will also accelerate their incorporation into commercial products.

This time frame, FY97 to FY02, will see the introduction of DGSA-consistent products through system reengineering and reacquisition. Older INFOSEC technologies will be eliminated at a greater pace. MISSI products will be in more widespread use. More DGSA-consistent products will be available and in greater variety from commercial vendors. Visionary fiscal planning and supportive budget execution are fundamental to gaining widespread DGSA-consistent product use. Efficient technology transfer and innovative acquisition strategies also will be key to the successful employment of DGSA-consistent products into systems.

Looking beyond FY02 the viewpoint on products begins to shift. More generalized, theoretical forecasts must be made. If one considers the product release cycle to provide a significantly new increment of functionality and performance at 12 to 18 month intervals, products released in FY95 should have undergone at least six significant evolutions. Increased demand for acquiring these newer products could probably have significant effects on the inventory of fielded products. Most of the DGSA-consistent products that resulted from successful research projects initiated in FY95 and earlier should be fairly well represented in the fielded inventory, many could have experienced significant upgrades. Those prototype products resulting from research initiated in FY96 to FY99 should be evolving into commercial products through various technology transfer processes and perhaps some could be in the early stages of field deployment. Those research projects that were initiated in the FY00 time frame could be moving into the prototype and advanced technology demonstration phase. Undoubtedly, new computing and communications technologies will have emerged causing a significant review in the solutions to achieve DGSA-consistency in fielded systems.

7.3 Transition Approach

The DGSA approach makes INFOSEC a user-driven requirements process that most importantly places the demand for appropriate products and supporting processes on the acquisition managers and their supporting techbase. Starting from a user-driven, mission-oriented approach, the abstract evaluation criteria and its supporting processes gain new meaning. The entire set of INFOSEC processes becomes tied to a system security engineering process that is part of the larger, overall system engineering process which must produce mission-oriented solutions. That is, individual processes now have a more appropriate framework within which to operate and be measured. The key difference is the starting point established by the DGSA.

With this new starting point, the DGSA provides technology pointers (e.g., separation technology, security protocols, and security management) so that research and development

(R&D) can begin on important components that must eventually be incorporated into products. The DGSA provides a clearer role for MISSI technology evolution and use in products. Standards can begin to exert an influence at the outset of R&D to ensure appropriate interface considerations are taken to achieve ease of technology transition, product assessment, system integration, and system interoperability. The DGSA also provides the basis for structuring INFOSEC E&T curricula to include focused awareness courses that can be delivered directly to commercial product vendors in order to promote technology transfer.

INFOSEC products are not widely available as mainstream commercial products. Demand generally must precede supply to provide commercial viability and such demand must be demonstrated in near and long term acquisition activity. To ensure that demand is adequate to maintain supply, the supplied INFOSEC products should fulfill the dimensions stated below. Today's products do not meet these dimensions and, therefore, provide weak incentives to acquisition activities.

The approach taken in the last decade to promote widespread availability of COTS products has not been successful in producing the type or range of products that are needed now. A new approach to INFOSEC technology transfer is needed. This approach should be to develop through internal NSA research, sponsored research, and technology partnerships, R&D proofs of concept that can serve as exemplary technologies for INFOSEC products. These technologies should have an end-user, mission, management, and overall architectural point of view. This approach should strongly leverage E&T of COTS product vendors as a primary method of technology transfer. The approach should also include providing partnered, commercial vendors a means to exploit exemplary technologies. Such means should include standardized interfaces that enable incorporation of the technology into other vendors' product lines to increase product availability. This approach should evolve to concurrently engineer the INFOSEC technologies with emerging computer technologies, products, and production processes in a manner that will gain rapid availability, cost efficiency, and high assurance with less risk.

There are many dimensions to the INFOSEC products problem. The six discussed in Table 7-2 are the most significant with respect to DGSA transition. COTS products that do not score high in each of these dimensions will most likely not provide the INFOSEC solutions required by the DGSA.

7.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 7.4.4. Subsection 7.4.5 provides the status of each segment task.

Dimension	Problem Description
Relevancy	INFOSEC products must support current and evolving computing technologies. INFOSEC products must be deployed within the state of computing practices and should remain close to state-of-the-art computing. Each INFOSEC product must provide a flexible assortment of protection functionality and strengths that can be optionally selected as part of the product's configuration either at acquisition time or at installation time. Key among the functions to be provided are: security management, cryptography, identification & authentication, information domain separation, and support for multiple policies.
Interoperability	INFOSEC products must provide the features necessary to construct integrated and interoperable systems. Such an integrated and interoperable focus can best be obtained from a general systems architecture (e.g., DGSA) which provides the basic protection concepts and principles to be embodied throughout the system. Mechanisms derived from this focus will provide the necessary protection features within a standardized framework of flexibility that allows for scalability and customization while promoting a basis for integration and interoperability (e.g., standardized mechanism interfaces and generalized protection mechanisms with selectable, parameterized protection features).
Affordability	INFOSEC products must be affordable both from an acquisitions and from an operational point of view. The products should not require costly acquisition procedures. The products acquired should have both reasonable purchase and upgrade costs. The products should also target to minimize the manpower burden required to provide system security management.
Efficiency	INFOSEC products must be efficient. Inefficient products will destroy demand or promote unsafe use of such products. The efficiency cost of INFOSEC to operational processing should be targeted at 5% or less than the efficiency cost of the same product without INFOSEC. The INFOSEC efficiency costs should not exceed 10% without explicit recognition that security is the overriding factor in the product's efficiency equation. Security management should not impose an unacceptable burden in terms of time or administrative overhead on the operational user. The products should provide protection defaults to ensure ease of secure use.
Effectiveness	INFOSEC solutions that are incorporated into COTS products must counter perceived threats by providing additional protection barriers or closing known or perceived system vulnerabilities. One solution does not fit all threat conditions. Therefore, COTS INFOSEC products must provide the ability to modify or tailor their INFOSEC solution to allow protection mechanism additions or to allow replacement of a weaker protection mechanism with a mechanism of greater strength and/or protection flexibility. Such modifiability shall not weaken the protection effectiveness of the COTS INFOSEC product.
Scalability	INFOSEC solutions that are incorporated into COTS products must scale to very large information systems with a large number of users, a large number of end systems that are geographically dispersed, and information processing that is characterized by high volume, stringent throughput and response demands, and a very large number of unique applications.

Table 7-2 Dimensions of INFOSEC Products Problem

7.4.1 Task 1: Current, Near-Term, & Long-Term Product Assessments

The objective of this task is to assess the quantity and type of DoD information systems and their associated INFOSEC products, now and in five and ten years, in order to develop implications for the marketability of INFOSEC products. The task involves gaining knowledge of the installed base of information processing and INFOSEC products so that assessments can

be developed with regard to INFOSEC product introduction timing, overall quantities required, and product appropriateness (i.e., DGSA-consistency, ability to support integration and interoperability, operational efficiency, etc.). This product assessment information can subsequently be used by the CISS staff, INFOSEC professionals, system security architects, standards bodies, security officers, program managers, and industry through an on-line INFOSEC products database.

Subtask 1.1: Snapshot Of INFOSEC Products

Description: There is a need to understand the current status of INFOSEC products (available, under development, or proposed). This subtask will capture a snapshot of representative products across the range of architectural components. This information will be captured in the products database. A representative sample of INFOSEC products to be included in the products database is provided in Appendix A. The products database will also include a synopsis of whether a representative product is, or can be made to be, DGSA-consistent from a concepts and principles perspective. Judgments of DGSA transition consistency will be based on: (1) the strength of domain isolation mechanisms including the ability to support multiple simultaneous instantiations of different information domains, (2) the ability to insert/integrate standard security management applications, information bases, and protocols as developed, and (3) the ability to integrate mechanisms that provide security association establishment and enforcement with trusted coupling of domain-executed security contexts. The representative view will be extended and coordinated during this task in order to populate the products database.

Responsible Organization: CISS Products Directorate and CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	R&T	Subtasks 1.1,1.3, 1.8,1.9, 2.2,3.2, 4.7,5.1	None
	SM	Subtask 2.1, Task 3,4,7	
	STD	Subtask 5.2	
	CN	Subtasks 4.2,4.3	

Required Staffing: 3 staff months 1995

Subtask 1.2: Inventory Of Installed Product Base

Description: This subtask requires identifying all computers (PCs, workstations, minis and mainframes) in the DoD inventory (including the Services). The mission areas (e.g., business, command and control, or intelligence) in which these computers are employed will also be identified. This identification will include the degree to which these computers are networked in LANs and wide area networks (WANs), and the types of operating systems and protocols that they employ. This information comprises the current or legacy product base. The near and long-term product base (five and ten years downstream) must also be forecast. NOTE: Barcode-based lifecycle inventory reporting could be investigated for use in maintaining this information.

Responsible agency: Primary: CISS Products. Support: DARIC.

Inter-task Dependencies: None

Required staffing: 12 staff months 1995

Subtask 1.3: INFOSEC Product Transition Market Planning

Description: This subtask requires identifying marketing implications for security products (i.e., the types of security products that are or will be needed, and an assessment as to their availability). Additionally, an assessment of major system acquisition programs product procurement plans and vehicles is required to provide information on the future dynamics of INFOSEC products in the installed base.

Responsible agency: CISS Products Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	R&T	Subtasks 1.1,1.3, 1.8,1.9, 2.2,3.2, 4.7,5.1	None
	SM	Subtask 2.1, Tasks 3,4	
	STD	Subtask 5.2	
	CN	Subtasks 4.2,4.3	

Required staffing:	6 staff months	1995
	6 staff months	1996
Total	12 staff months	

7.4.2 Task 2: Products Database

The objective of this task is to promote information exchange and coordination. The INFOSEC products segment team will focus on this objective in providing an available, on-line, centrally coordinated source of existing and planned INFOSEC product information to the CISS staff, INFOSEC professionals, system security architects, standards bodies, security officers, program managers, and industry. This task involves the creation of a products database to enhance INFOSEC information coordination and exchange. The product database will list all currently available products, along with those under development and those expected to be developed. The database will have an electronic interface allowing easy access.

Subtask 2.1: Develop Products Database

Description: This subtask entails the creation of the database. The database has already been designed to accommodate a wide range of INFOSEC product information including the following: vendor information, product description, target applications, availability, cost, interfaces, security services and mechanisms, product features, and documentation references. The structure for the database entries has been defined and the necessary, initial interfaces created.

Responsible Organization: CISS Products Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	R&T	Subtasks 1.1,1.2, 1.3,1.8, 1.9,2.2, 3.2,4.7,4.8,4.9,5.1	CN	Subtask 4.3
	SM	Subtask 2.1, Tasks 3,4,7	LSE	Tasks 3,5,7,8
	STD	Subtask 5.2	SM	Task 11
	CN	Subtask 4.2	E&T	Subtask 3.1

Required Staffing:	6 staff months	1994

Subtask 2.2: Populate Products Database

Description: The products database must be populated with information on existing products, products under development and products that are being planned. The initial sources of this data have been industry marketing literature and other open-source documents such as NSA's Evaluated Products List (EPL). Included in the Products Database will be: product security profiles from the NSA ISSO; Services' product assessments; defense agencies' tested results; program manager's statements of Government experience with deployed products; product evaluations electronically received from NSA's Trusted Product Evaluation Program; and INFOSEC product data from NSA's Network Security Products Division and NSA's Network Security Infrastructure Division.

Responsible Organization: CISS Products Directorate.

Inter-task Dependencies: Same as Subtask 2.1

Required Staffing:	13 staff months	1994
	6 staff months	1995
	6 staff months	1996
	6 staff months	1997
	6 staff months	1998
	6 staff months	1999
Total	43 staff months	

Subtask 2.3: Enhance Products Database

Description: After the products database becomes operational, the CISS Products Directorate will elicit comments and suggestions for improvement of the database and the user's manual. There are potentially many extensions or linkages to the products database that could support the DOTS effort. General database linkage mechanisms will be investigated as part of these enhancement . These enhancements to the database will complement the development of the electronic catalog.

Responsible Organization: CISS Products Directorate.

Inter-task Dependencies: Same as Subtask 2.1

Required Staffing:	2 staff months	1994
	12 staff months	1995
	6 staff months	1996
	6 staff months	1997
	6 staff months	1998
	6 staff months	1999
Total	38 staff months	

Subtask 2.4: Develop And Make E-Catalogue Available

Description: An electronic interface will be developed for the product database. The electronic interface will allow "on-line" interaction with the product database.

Responsible Organization: CISS Products Directorate.

Inter-task Dependencies: None

Required Staffing: 12 staff months 1995

Subtask 2.5: Link With Security Service Mechanisms Catalog

Description: This subtask requires linking the INFOSEC products database with a database of security service mechanisms (automated, physical, personnel, or procedural) that are requirements of current and planned programs in the Defense Information Infrastructure (DII). The objective is to identify where products have been used or will be used to satisfy known requirements. Security service mechanisms currently in R&D will be included in this database, with a description of their intended functionality and an estimated initial operational capability. Linkage mechanisms will be determined in conjunction with the R&T segment.

Responsible Organization: CISS Products Directorate with support from the R&T segment and various OSD program managers (e.g., DISN, DMS, et al).

Inter-task Dependencies: None

Required Staffing:	12 staff months	1995
	12 staff months	1996
Total	24 staff months	

7.4.3 Task 3: INFOSEC Products Procurement Vehicle

Description: The objective of this task is to examine the various acquisition vehicles for INFOSEC products and to determine if a more suitable set of acquisition vehicles needs to be developed. If such development is required, the INFOSEC products segment would coordinate the activities to provide DoD INFOSEC customers with an efficient, economical contract vehicle by which they could obtain INFOSEC product support for products described in the products database. Such a contract could also provide an avenue by which MLS solutions that are prototyped and assessed in the DoD MLS Demonstration and Assessment Center could be fielded. This procurement vehicle would provide CISS with the ability to oversee the requirements and flow of INFOSEC products to DoD customers (similar to INFOSEC Technical Services Contract) and would provide a "one-stop" INFOSEC procurement support organization for all of DoD. Further, it would address vendor concerns about DoD markets for INFOSEC products and could provide incentives for vendors considering secure product releases.

Responsible Organization: Primary: CISS Products Directorate. Support: CISS IP3, MLS Products, NSA X, various OSD program managers (e.g., DISN, DMS, et al), and GSA.

Inter-task Dependencies:	Input Dependencies		OUTPUT DEPENDENCIES
	R&T	Subtask 1.9	None
	SM	Tasks 11,13	
	LSE	Tasks 3,6,7,8	
	CN	Subtasks 4.2,4.3	

Required Staffing:	9 staff months	1995
	3 staff months	1996
Total	12 staff months	

7.4.4 Resource Summary and Transition Schedule

Table 7-3 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 7-1 shows the segment transition schedule.

	Resources Required in Staff Months						
Tasks	1994	1995	1996	1997	1998	1999	Total
1.1		3					3
1.2		12					12
1.3		6	6				12
2.1	6						6
2.2	13	6	6	6	6	6	43
2.3	2	12	6	6	6	6	38
2.4		12					12
2.5		12	12				24
3		9	3				12
Total	21	72	33	12	12	12	162

Table 7-3 Products Segment Summary of Required Staff Resources

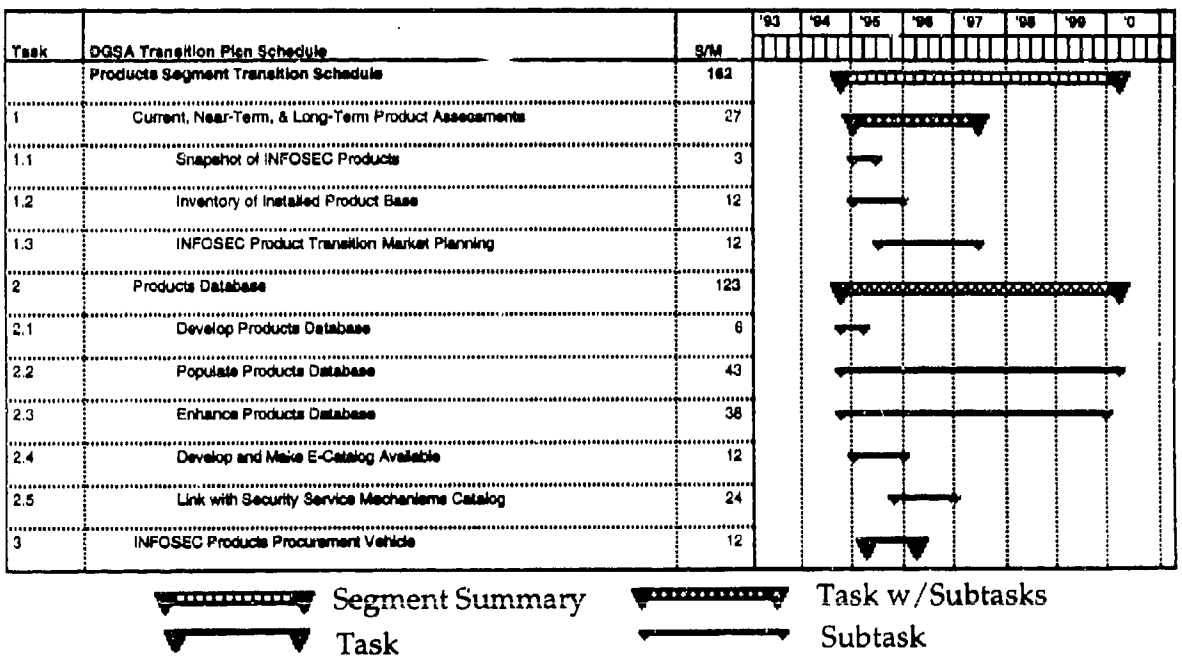


Figure 7-1 Products Segment Transition Schedule

7.4.5 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

Task 2.1 Develop Products Database

This task is underway by the CISS Products Directorate with expected completion this year.

Task 2.2 Populate Products Database

Work is underway to start to populate the Products Database.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1.1, 1.2, 1.3, 2.3, 2.4, 2.5, and 3 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

8. LOCAL SUBSCRIBER ENVIRONMENT SEGMENT TRANSITION STRATEGY

8.1 Introduction

The Local Subscriber Environment (LSE) Transition Strategy addresses the concerns for the LSE area with respect to transitioning toward the DGSA. The LSE is defined by the DGSA as all computer and communications systems under administrative control of a single organization. To realize this, the DGSA will require that current and future LSEs incorporate the concepts of the DGSA. The DGSA reflects a significant architectural decision regarding the allocation of security functions. The LSE will assume most of the responsibility for providing information security. Therefore, new LSE architectures, in many cases tailored for specific uses, must be developed with the goals of the DGSA in mind. Existing systems should be examined to identify opportunities to incorporate DGSA principles during their life cycle.

The LSE segment must provide an approach for transitioning the LSEs toward the DGSA objectives. That is, this segment will develop planning strategies to allow the LSE program managers to work toward the achievement of the DISSP security goals. Guidelines for the incorporation of new products and existing products (e.g., firewalls and integrated I&A functions) to produce DGSA-based security architectures will be developed by the LSE segment. This transition strategy also includes an approach for providing information system program managers with the necessary DGSA-related standards, products, and research and technology information.

8.2 Background

For years the community has operated without a well-formed plan that would provide for the continuous, cost-effective development of security solutions. Today, mission planners seek to take advantage of increased information system capabilities to produce more successful results, but are constrained by the lack of effective information system security solutions and poor planning. The present day situation leads to cumbersome and ineffective near-term approaches. Security solutions are a reaction to technology, and more often than not, an add-on to systems after development. Technology continues to advance so rapidly that security products are often rendered obsolete by the time they are deployed. Products currently under development will fall short of the future mark under today's security development strategy. The effect is costly, inappropriate, and in some cases, unusable security products.

The DGSA provides guidance in a process that will correct past and current deficiencies in secure information processing. It presents a flexible and evolutionary plan consistent with open systems and other driving focuses of the DoD TAFIM and Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) [10]. The DGSA is a generic architecture from which mission specific security architectures can be derived and as a goal, ensures that they are consistent with future mission needs and evolving technology. Specific information system architectures will require transition plans for achieving the DGSA objectives where current technologies do not meet all the security requirements of a mission.

8.3 Transition Approach

The two most significant issues confronting the LSE segment are how to apply the DGSA to the development of system security architectures in the near-term and the availability of products and technologies over the long-term to realize the security concepts articulated in the DGSA. The first issue is addressed through the development of guidance documents by the LSE segment. The LSE segment transition strategy calls for the development of architectural guidance to assist system security architects in incorporating the DGSA into their architectures

based on currently available technologies. The LSE segment will establish the security requirements of the thirteen functional areas within the DoD (distribution, environment, finance, health, human resources, information management, material resources, procurement, reserve components, transportation, command and control and intelligence). Based on these requirements, migration architectures for each of the functional areas will be developed and incorporated into the DGSA as appendices. The LSE segment will develop similar guidance and migration architectures for the mid-term to facilitate the incorporation of the DGSA concepts. The LSE segment will also address how to define and apply doctrinal mechanisms to satisfy a portion of the security requirements incorporated in architectures. Where possible the LSE segment will leverage off of existing documents which address the near and mid-term such as the DII Master Plan.

The second issue must be addressed in two parts. Too often, the community has developed products without fully understanding the user's requirements and without considering their utility in the overall system security architecture. The LSE segment tries to amend both of these problems. First, the segment will focus on capturing the security requirements across the DoD community through the development of a system profile database. The system profile database will document the mission, its requirements, and the architectural solution developed for that mission. The LSE segment will work with the system security architects to identify which of these requirements cannot be satisfied with existing products or which products would be useful to enhance the overall security of the system. Finally, the LSE segment team will work with the Products and R&T segments to develop an approach for transitioning these requirements from concepts to prototypes and finally to Commercial-Off-The-Shelf (COTS) products.

There are two major transition points for the LSE segment: the development of the requirements transition process and the completion of the near-term guidance documents. Each of these transition points moves the community closer to the implementation of DGSA based local subscriber environments.

Part of the LSE transition approach is the development of a system profiles database. The database for each system will include a mission description, the list of user requirements and the architecture that was developed to meet those requirements. Additionally, the database will capture those requirements which could not be effectively satisfied by existing products and standards. The LSE transition approach envisions representatives of the products, standards, and R&T communities working with the LSE segment to develop a process for translating those requirements into COTS products. This process will have multiple elements. It will provide a means for vendors to demonstrate an established customer base for specific products. It will allow the R&T community to focus and prioritize research efforts based on user requirements. It will be a major transition point for the LSE segment once this process has been defined and implemented.

One of the criticisms of the DGSA is that it does not address the near-term problems that are facing the DoD community. One of the elements of the LSE transition strategy is to combat this criticism by developing near-term architectures which satisfy the requirements of the 13 functional areas within the DoD enterprise model. These architectures will show what can be accomplished today towards implementing DGSA based architectures. Additionally, a guidance document will be produced which will assist architects in developing their own DGSA based architectures to satisfy their mission requirements. It will be a major transition point for the LSE segment, once the DoD community recognizes that the DGSA addresses their problems and has utility for the near-term.

8.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required t carry out these tasks are part of existing activities. These activities are included as part of this s nent strategy. A resource summary and transition schedule for the segment is presented in Subsection 8.4.10. Subsection 8.4.11 provides the status of each segment task.

8.4.1 Task 1: Establish CFII Linkage

Description: Completing the tasking in this segment will require a close linkage between CFII and CISS A&E. This task will look at how the organizations can support one another and how to accomplish the tasking outlined in this segment.

Responsible Organization: Enterprise Integration and CISS A&E

Inter-task Dependencies: N/A

Required Staffing: 6 staff months 1995

8.4.2 Task 2: Establish Security Requirements for 13 Functional Areas

Description: CFII is in the process of developing near-term architectures and migration strategies for the thirteen functional areas that CFII has defined. Those areas are distribution, environment, finance, health, human resources, information management, material resources, procurement, reserve components, transportation, command and control and intelligence. It is important that these architectures embody the concepts of the DGSA where possible. DGSA concepts and principles will be difficult to insert completely into the near-term strategies, but will be critical for follow-on migration. Paramount to this task is the system analysis required to understand the functional area organizations, their business flow, and the identification of uniquely sensitive categories of information. This analysis, and a subsequent threat analysis of each unique sensitivity category of information is necessary in order to develop appropriate security policies for the functional areas. This will constitute over 75% of the work on this task. The other 25% of the work will entail the development of the 13 functional area security policies.

Responsible Organization: CFII and CISS / &E lead a joint effort, which will also include individuals from the NSA DII support organization (V33).

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Prod	Task 2	N/A
	CN	Subtask 4.1	
	Policy	Subtask 5.1	
Required Staffing:	90 staff months	1995	
	90 staff months	1996	
Total	180 staff months		

8.4.3 Task 3: Short Term Guidance (1-3 yrs)

Description: The DGSA provides a goal architecture. This task will generate and maintain a target security architecture, based on the DGSA, that is focused on the capabilities available in the near-term. This will provide guidance for architects developing architectures for the near-term. Part of the guidance will be an assessment of the products available in the near-term, this will be provided to the products segment for incorporation into the products database. This task will utilize existing documents, such as the DII Target Security Architecture, as input in the development or the identification of existing guidance documents.

Responsible Organization: CISS A&E and DISA CFSE

Inter-task Dependencies:	Input Dependencies	Output Dependencies
	CN Subtask 3.1	

Required Staffing:		
	36 staff months	1995
	36 staff months	1996
Total	72 staff months	

8.4.4 Task 4: Generic Architectural Guidance

Description: Generic architectural guidance is needed so architects can understand how to incorporate the DGSA into architectures that they are developing. This task will complement the work being accomplished in Task 3 by developing representative architectures based on the mission requirements of the functional areas. These will serve as an example for architects as they develop their own architectures. The representative architectures developed in this task will be added as annexes to the DGSA.

Responsible Organization: Primary: CFSE. Support: CISS A&E and NSA DII.

Inter-task Dependencies: N/A

Required Staffing:		
	60 staff months	1995
	60 staff months	1996
Total	120 staff months	

8.4.5 Task 5: Establish Systems Profile Database

Description: To support architects in the development of mission specific architectures, a systems profile database will be needed. The database will capture the systems profile work being done at NSA. The database will also contain the mission-specific architectures that are being developed. These entries will not only describe the architectures, but any requirements that the architects were not able to meet due to technology or the requisite products being unavailable. Architects will be able to utilize the system profiles and the mission specific architectures to develop their own architectures. The R&T Segment will be able to review those requirements that were not satisfied to initiate the necessary research. The Products Directorate will be able to review the database to determine what products are not available and, if there is a broad enough base, try to get vendors to develop the necessary products.

Responsible Organization: Primary: CISS A&E. Support: CISS Products Directorate, systems profiling and research and technology organizations.

Inter-task Dependencies: N/A

Required Staffing:	60 staff months	1995
	60 staff months	1996
Total	120 staff months	

8.4.6 Task 6: Process Definitions Guidance

Definition: A process needs to be institutionalized to support the transition of architectural requirements to COTS products. The first step in establishing that process is to write a document which outlines the intended process. This guidance document will be written jointly by CISS Architecture & Engineering (A&E) and the CISS Products Directorate. The process described in Task 5 will rely heavily on the Systems Profile Database being developed in Task 5. The document will define the format and expected content of the mission specific architectures. The document will also outline the responsibilities of the CISS A&E, the CISS Products Directorate and the research and technology organizations in the development of products.

Responsible Organization: DISA CFSE and CISS Products Directorate

Inter-task Dependencies: N/A

Required Staffing:	12 staff months	1995

8.4.7 Task 7: Mid-Term Guidance (4-6 yrs)

Description: This task is a continuation of the work that was accomplished in Task 3, but the focus will be on the mid-term. The result will be a goal architecture which makes use of the anticipated security products/components that will be available during this time frame.

Responsible Organization: Primary: CISS A&E. Support: CFII and NSA DII organization.

Inter-task Dependencies: N/A

Required Staffing:	120 staff months	1996
	60 staff months	1997
Total	180 staff months	

8.4.8 Task 8: Specific Architectural Guidance

Description: This task is a continuation of the work that was accomplished in Task 4. This task will complement the work that is being done in Task 7 and will develop example architectures based on specific mission requirements for the mid-term. This task will outline the process from the analysis of the mission requirements to the creation of an architecture. The task will result in a document which will provide valuable guidance to architects.

Responsible Organization: Primary: DISA CFSE. Support: NSA DII and system profiling organizations.

Inter-task Dependencies: N/A

Required Staffing:	90 staff months	1996
	90 staff months	1997
Total	180 staff months	

8.4.9 Task 9: Doctrinal Architecture Design Guidance

Description: This task will provide guidance on how to define and apply doctrinal mechanisms to satisfy a portion of the security requirements incorporated in architectures. This task will focus on the full range of doctrinal mechanisms and how to assess the relative strength of the mechanisms. This task will leverage off of any recommendations made in the JSC report. The task will produce a guidance document at its conclusion.

Responsible Agency: DISA CFSE

Inter-task Dependencies: N/A

Required Staffing: 60 staff months 1995

8.4.10 Resource Summary and Transition Schedule

Table 8-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 8-1 shows the segment transition schedule.

	Resources Required in Staff Months			
Tasks	1995	1996	1997	Total
1	6			6
2	90	90		180
3	36	36		72
4	60	60		120
5	60	60		120
6	12			12
7		120	60	180
8		90	90	180
9	60			60
Total	324	456	150	930

Table 8-1. LSE SEGMENT SUMMARY OF REQUIRED STAFF RESOURCES

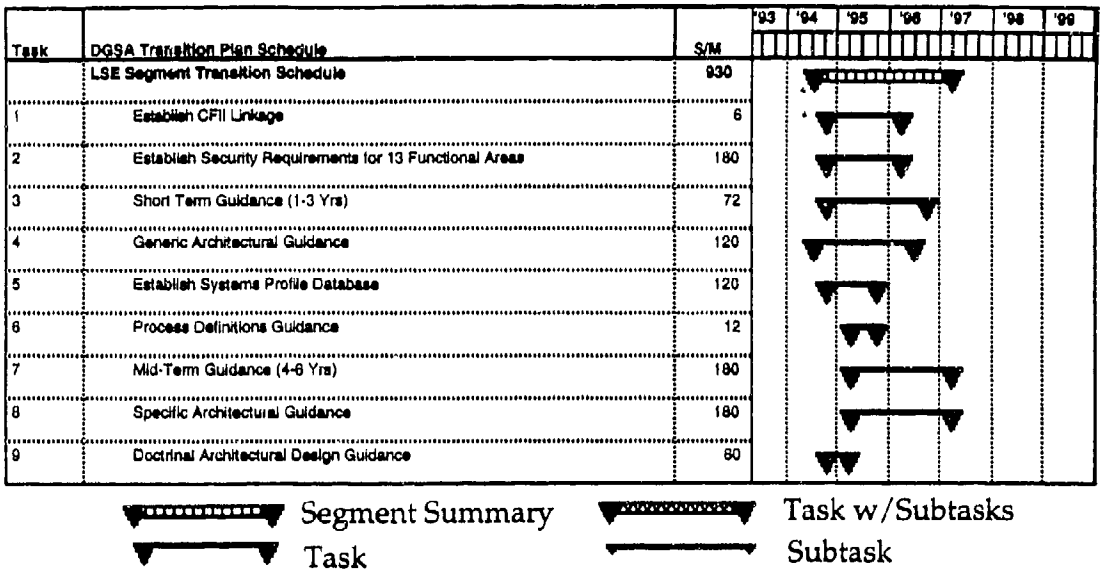


Figure 8-1 Local Subscriber Environment Segment Transition Schedule

8.4.11 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

Task 3 Short Term Guidance

CISS A&E plans to start this task in second quarter FY95.

Task 4 Generic Architectural Guidance

CISS A&E plans to start this task in second quarter FY95.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1, 2, 5, 6, and 9 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

(This page is intentionally blank.)

9. STANDARDS SEGMENT TRANSITION STRATEGY

9.1 Introduction

The Standards Segment transition strategy describes the role of standards in transitioning toward the DGSA. In particular, this strategy provides a brief introduction to the standards segment and the segment goals with respect to the DGSA; background information on current security standards activities; the standards transition approach; and the tasks that need to be accomplished in the transition process. The goals of the Standards Segment are: (1) to promote the availability of security-related standards to support the DGSA in the transition of existing systems and in the development of new systems, (2) to identify areas requiring security standards that are not being addressed by available or emerging standards, (3) to identify ways to address standards shortfalls, and (4) to prioritize and provide a rationale for security standards activities.

To accomplish its goals, the Standards Segment is organized in a two-tiered structure. The first tier is an ad hoc steering group, the Security Standards Transition Team (S2T2). The S2T2 includes representatives from the DISA Center for Standards (CFS), DISA CISS, DISA Joint Interoperability Test Center (JITC), NSA, and the National Institute of Standards and Technology (NIST). The S2T2 reviews standards transition products, assists in standards transition work efforts, and directs and guides standards transition planning. The second tier, the Security Standards Transition Subgroup of the Information Systems Security (INFOSEC) Standards Working Group (ISWG), chartered under the DoD Standards Coordinating Committee (SCC) provides coordination assistance. The S2T2 and the Security Standards Transition Subgroup are chaired by the Standards Segment Leader from DISA CFS.

9.2 Background

DISA, as the DoD Executive Agent for information technology standards, coordinates the development and adoption of standards within DoD and externally by soliciting DoD participation in the information technology management process. This process includes the standards management committees and working groups responsible for developing, selecting, managing, and approving information technology standards for a particular area, such as security. The DoD standards management committee or working group for a particular area establishes the DoD position, or guidance package, for a DoD representative to take to international, federal, or commercial standards bodies. DISA CFS, per a request for participation by CISS, is working to increase DoD representation and influence within international, national, and commercial standards bodies.

On 29 June 1994, the Secretary of Defense issued a memorandum on the subject of "Specifications and Standards - A New Way of Doing Business" [11]. This memorandum established the use of performance specifications in lieu of military specifications and standards, allowing the latter only as a last resort and with an appropriate waiver. Where performance specifications are not practical, non-Government standards are to be used. The memorandum calls for development of specification language that will encourage contractors to propose non-Government standards and industry-wide practices for both requests for proposals and on-going contracts. Outdated military specifications, standards, and data requirements are to be identified and removed. Where practical, non-Government standards are to be developed to replace military standards. Many other changes were also stipulated in this memorandum. The full impact of this memorandum is still being assessed. It appears that the Standards segment will need to focus on inserting DGSA changes into non-Government and Federal standards.

Numerous security-related standards exist or are in various states of development. The "Survey of Available and Ongoing Security Standards and Products" [12] provides a list of the

currently available and emerging non-Governmental, federal, and DoD, security-related standards. For each standard listed, the survey document also provides the sponsor, status, functionality, and, where known, the availability of any products implementing the standard.

As noted in "DGSA Security Standardization Areas" [13], the DGSA is oriented toward future information systems and focuses on both users and information. The DGSA perspective of distinct autonomous information domains that are distributed among networked computer systems is vastly different from previous treatments of INFOSEC. [13] examines security standards from this DGSA perspective to "...establish a taxonomy appropriate for all security standards, review those areas of standardization directly stated within the DGSA document, and identify areas of standardization drawn from the DGSA that are not currently being addressed by standardization bodies." Table 9-1, reproduced from [13] summarizes the set of standardization areas identified by the DGSA, including the security principles and associated technology areas.

Principle	Technology Area	Standardization Area
Strict Isolation	Separation Kernel	Programming Interface
	Security Critical Functions	Elements of Management Information
	Protection Mechanisms	Techniques Elements of Management Information
Decision/ Enforcement Separation	Security Policy Representation	Elements of Management Information Methods (for formulating policy decision rules)
Constrained Dispersion [13]	Transfer System	Protocols (Security Protocols) Elements of Management Information
Security Management	Systems Management	Protocols (Management Protocols) Elements of Management Information Programming Interface (Generic Security Services Application Programming Interface (GSSAPI))
	Key Management	Protocols (Security Association Management Protocols) Security Information Objects Techniques Elements of Management Information
Absolute Protection	Protection Mechanisms	Methods (for [illegible] of mechanism) Registration (of [illegible] mechanisms)
Uniform Accreditation	Certification and Accreditation	Guidance

Table 9-1. Summary of Core Standardization Areas

"A Mapping of Standards and DGSA Standards Requirements" [14] provides an assessment of security standards relative to DGSA requirements, as defined by [13], against current and emerging standards, as defined by [12] and other sources of information. The report characterizes standards as generic, mission-specific, deficient, or interim solutions. Generic standards solutions will address a broad range of DGSA-compliant systems. Mission-specific standards solutions address a distinct set of mission-specific standards leading toward the DGSA. Deficient standards solutions provide only part of the required DGSA functionality [Ref]. Interim standards solutions may not agree with the DGSA, but provide needed functionality until DGSA-compliant standards are developed. If no useful standards are available, the standardization area is deemed as having a gap. The findings of the mapping document are summarized in Table 9-2.

Principle	Technology Area	Standards Area	Status
Strict Isolation	Separation Kernels	Programming Interface	Deficiency
		Guidance Standards	GAP
	Security Critical Functions	Elements of Management Information	Deficiency
	Multi-Domain Objects	User Interface	GAP
		Guidance	GAP
Decision and Enforcement	Security Policy Representation	Methods (for Policy Representation)	GAP
		Elements of Management Information	Deficiency
Security Management	Systems Management	Security Management Protocols	COMPLETE (emerging)
		Elements of Management Information	UNKNOWN
		Programming Interface	UNKNOWN
Absolute Protection	Protection Mechanisms	Measures (for expressing the Strength of Protection Mechanisms)	GAP
		Registration of Protection Mechanisms	GAP
Uniform Accreditation	Certification and Accreditation	Guidance	GAP
		Meta-Standards (Criteria) and related standards	Deficiency

Table 9-2. Summary of Standardization Areas Deficiencies and Gaps

9.3 Transition Approach

The Standards Segment transition approach includes developing standards guidance for the evolutionary implementation of the DGSA. The effort requires identifying areas not being addressed by emerging or available standards and identifying ways to satisfy these areas. The standards approach will help prioritize and provide a rationale for security standards activities. The standards approach to transition follows a seven-step process as illustrated in Figure 9-1. These steps are: 1) define requirements, 2) establish a baseline, 3) identify shortfalls, 4) plan work on the shortfalls, 5) conduct the work on shortfalls, 6) document the work, and 7) establish a new baseline. This basic process follows an iterative approach similar to a rapid prototyping system engineering approach. This approach defines a process that can be institutionalized by the organizations that will eventually take over the standards activities.

As described in Section 9.2, the first iteration of steps 1 through 3 in the process have been completed. The remaining steps are in various stages of completion. In order to determine what standards activities are needed to address the shortfalls identified in the earlier steps, an action plan is being developed. In addition to describing the standards activities needed, this action plan will list the expected timeline for starting and completing work, the priority of the activity to the DGSA, the estimated resources, and the recommended DoD standards working group and standards development organization. As the standards activities are identified, the Standards Segment will "hand off" responsibility for accomplishing those efforts to formal organizations, such as the DISA CFS. The Standards Segment will also provide recommendations for security related standards and iteratively update the transition planning, highlighting the products developed under the steps previously described. The Standards Segment is also investigating the

best approach for ensuring the work products and processes, including standards development activities, are institutionalized into the formal organizations such as DISA CFS. As mentioned before, this is an iterative process dependent upon any changes in status of available and emerging standards and the initiation of new standards development activities. Also, the DGSA security standards requirements may change based upon revisions to the DGSA. Any change to this initial step in the Standards Segment transition strategy will impact the remaining steps.

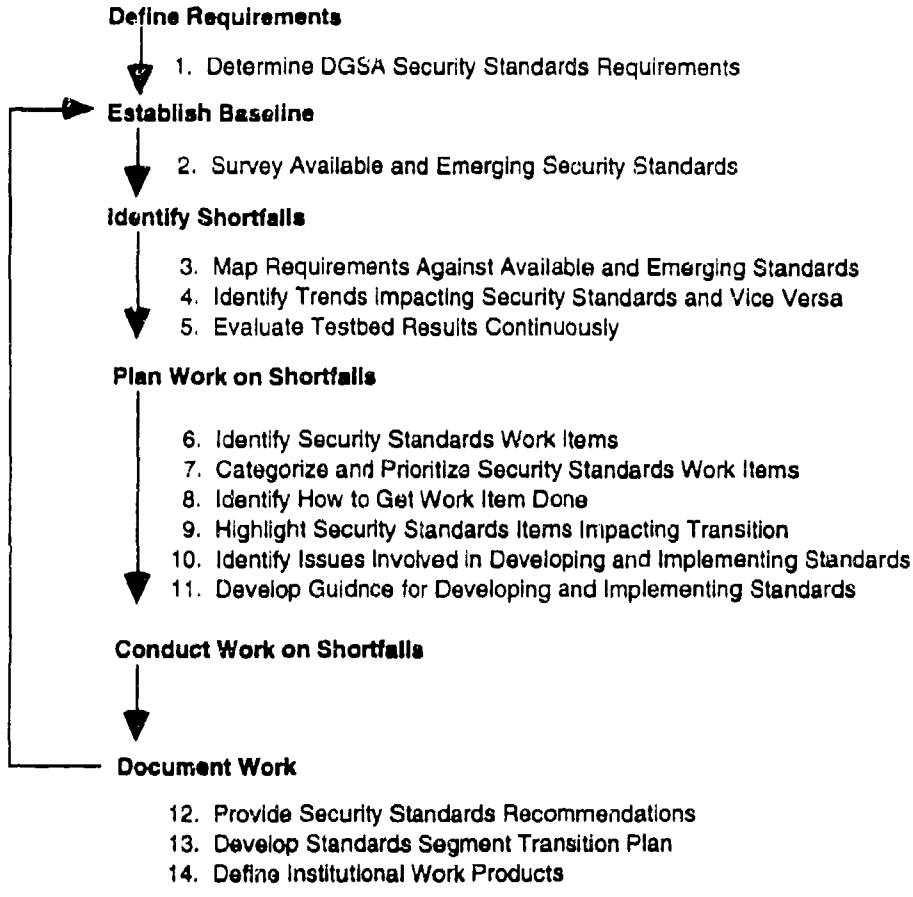


Figure 9-1. Steps in the Standards Transition Process

This transition strategy will benefit all agencies of the U.S. Government, (e.g., DoD, DISA CISS), as well as commercial enterprises in the private sector. Benefits are achieved by promoting the availability of standards to fulfill the DGSA standardization requirements and provide the structure and guidance for incorporating security standards into open systems to promote integration, interoperability, and a common baseline for developing security standards. Cost savings will be achieved by encouraging the adoption of security standards in COTS products. As the DGSA notes, "Particularly in the face of current budgetary constraints, it is highly desirable that security features become standard elements of COTS or GOTS equipment so that security has minimal impact on price." Three strategies that will show valuable long-term benefits from standardization are portability of applications via standard interfaces, reuse of software components via identification of standard processes and modularization, and reuse of C&A results via standard C&A processes and documentation.

There are four major transition points for standards, as previously shown in Figure 2-1. The first, a survey of all security standards will be complete and available in FY 1995. The second major transition point will occur in FY 1997. At this point, the baseline showing where all the gaps and shortfalls in standards are, with respect to the DGSA requirements, should have been identified. Some form of database (manual or automated) will have been created containing all standards survey and analysis information. The third major transition point will occur in FY 1999. The initial phase of many of the standards activities will be complete. All standards and guidance in support of the separation kernel should be available in an early draft stage. The initial versions of criteria, standards, and guidance for the new C&A process will be complete. Similarly, the representation methods and guidance for security policies will have completed the initial phase of development. Both security policy and security management tasks will be underway. The definitional activities in support of security management will also have completed an initial phase, although the standards in this area will not be complete. Finally, new metrics for security mechanisms will be standardized, along with a technique for registering such mechanisms. The fourth major transition point for Standards will occur in FY 2001. All major revisions to the DGSA that could have an impact on standards will be complete. Responsibility for the standards tasks will have shifted to the responsible formal organizations. Any additional activities identified after the beginning of this effort, requiring standards support, will have been assigned to an appropriate organization.

9.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 9.4.8. Subsection 9.4.9 provides the status of each segment task.

9.4.1 Task 1: Separation Kernel Support

A separation kernel mediates all calls to security critical functions. Various types of standards will be necessary to support the development of end systems based on separation kernel technology.

Subtask 1.1: Separation Kernel Programming Interface

Description: A standard for a generic programming interface to the separation kernel will be developed based on the activities of the Research and Technology segment.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
	R&T	Subtask 1.1.6	
Required Staffing:	30 staff months	1997	
	30 staff months	1998	

	15 staff months	1999
Total	75 staff months	

Subtask 1.2: Separation Kernel Guidance

Description: For those DGSA systems that will use separation kernel technology, meta-standards or additional guidance will be required for the design and implementation of the kernels.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
	R&T	Subtask 1.1	

Required Staffing:	18 staff months	1997
	18 staff months	1998
	12 staff months	1999
Total	48 staff months	

9.4.2 Task 2: Security Critical Functions-Management Information Elements

Description: To support the management of security critical functions, object class definitions for separation kernels should be standardized. While existing standards address managed objects, they do not address objects unique to a separation kernel (e.g. objects that support the interface between the SPEF and SPDF). Such object definitions require that the programming interface and design guidance for separation kernels be complete.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,5	

Required Staffing:	22 staff months	1996
	22 staff months	1997
	22 staff months	1998
	14 staff months	1999
Total	80 staff months	

9.4.3 Task 3: Security Policy Support

The DGSA calls for the division of the decision and enforcement portions of the mechanisms enforcing policies. Such division requires that the decision and enforcement functions be independent. Using this technique, the enforcement functions have no knowledge of the specific policy being enforced and the decision functions provide the policy interpretation. This task requires the development of various types of standards concerned with security policies.

Subtask 3.1: Security Policy Representation Methods

Description: Some security policy components will be resident in the SMIB. At the current time, there are no standard or defacto standard approaches for the concise representation of security policies and security policy decision rules, nor for the SMIB itself. Security policy representation will require research prior to standardization.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,6, Subtasks 2.2,2.4	
	R&T	Subtask 1.1.4	
Required Staffing:	24 staff months	1996	
	36 staff months	1997	
	21 staff months	1998	
Total	81 staff months		

Subtask 3.2: Security Policy Representation Guidance

Description: After the methods for security policy representation have evolved, additional guidance will be required to explain the use of the policy representation methods.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1, Subtasks 2.2, 2.4	
	Policy	Task 5 and all Subtasks	
Required Staffing:	15 staff months	1996	
	15 staff months	1997	
	15 staff months	1998	
	12 staff months	1999	
Total	57 staff months		

Subtask 3.3: Security Policy Management Information Elements

Description: This task requires definition of the classes of objects specifically representing policies that will reside in the SMIB. A standard containing the policy object definitions will be provided.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,4,5	
	R&T	Subtask 2.2	

Required Staffing:	20 staff months	1996
	24 staff months	1997
	18 staff months	1998
Total	62 staff months	

9.4.4 Task 4: Security Management Support

System management directly involves security management. The DGSA looks toward integrating them more fully in the future. Two specific concerns related to security management information are the exchange of such information over the local and/or wide area networks and the definition of management objects that will reside in the SMIB. The DGSA requires that an information base (i.e., the SMIB) of all security relevant information (e.g., security management information) be maintained. The SMIB may include audit related information, encryption key information, security alarm information, policy information, registration information, and object security attribute information.

Subtask 4.1: Security Management Protocols

Description: SM application protocols are needed for exchanging security management information. A standard will be developed for these systems management protocols.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,4,9	
	R&T	Subtask 2.2	

Required Staffing:	24 staff months	1996
	24 staff months	1997
	14 staff months	1998
Total	62 staff months	

Subtask 4.2: Security Management Object Definitions

Description: A standard will be developed to include all object definitions for the SMIB, other than policy object definitions which are addressed in Subtask 3.3.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,6	

Required Staffing:	24 staff months	1996
	30 staff months	1997
	14 staff months	1998
Total	68 staff months	

Subtask 4.3: Security Management Related Standards

Description: This subtask supports related standards activities for security management. It includes standards for profiles, meta-standards, reference materials, and guidance.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	SM	Tasks 5,6.7,8,9,11
	SM	Task 1		

Required Staffing:		
	33 staff months	1995
	33 staff months	1996
	32 staff months	1997
	32 staff months	1998
	32 staff months	1999
	21 staff months	2000
Total	183 staff months	

Subtask 4.4: Security Management Registration

Description: The registration of techniques for key management will allow end systems to negotiate regarding the communication and transfer of information. Complete system management will include the registration of profiles. Some registration procedures already exist and could form the basis of approaches supporting the DGSA. A standard approach for registering profiles will be developed.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1, 7	

Required Staffing:		
	10 staff months	1996
	16 staff months	1997
	6 staff months	1998
Total	32 staff months	

9.4.5 Task 5: Security Mechanism Metrics and Uniform Accreditation Support

Security mechanisms must be considered in terms of their strength and required functionality, to determine their adequacy for supporting a given information domain. Mechanisms that can contribute to the support of a given information domain should be registered following evaluation for strength. Such registration will promote the reuse and proper use of existing security mechanisms. Such registration will also support a new uniform accreditation process. Uniform accreditation will require that the accreditation process for all systems is consistent. A standard for DGSA-consistent uniform certification and accreditation process will be developed.

Subtask 5.1: Security Mechanism Metrics

Description: This subtask requires standardization of the security mechanism metrics developed by the security management segment, in conjunction with the R&T segment. The security mechanism strength standards developed will define the process for determining mechanism strength and provide a set of metrics. This area requires research and development prior to any standardization activity.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Task 8
	SM	Task 1	C&A	Subtask 3.3
			SM	Task 7

Required Staffing:	7 staff months	1997
	8 staff months	1998
Total	15 staff months	

Subtask 5.2: Security Mechanism Registration

Description: This subtask requires the standardization of the security mechanism registration approach. The standard approach developed for security mechanism registration may draw upon existing approaches for mechanism registration.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Task 8
	SM	Task 1	C&A	Subtask 3.3
	STD	Subtasks 4.4, 5.1	SM	Task 7

Required Staffing:	6 staff months	1998
	3 staff months	1999
Total	9 staff months	

Subtask 5.3: Uniform Accreditation - Criteria, Standards, and Guidance

Description: The new criteria developed in support of uniform accreditation will need to provide a flexible foundation and specifications for separation mechanisms. New accreditation standards will need to address data sensitivity, system mechanism functionality, security mechanism assurance, operational environments, personnel security, systems evaluation, and risk management. Any additional guidance necessary to support the new uniform accreditation process will also need to be developed.

Responsible Organizations: DISA CFS or other Government standards organization.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Tasks 1,4	LSE	Task 8
	SM	Task 1	C&A	Subtask 3.3
	C&A	Subtasks 3.1, 3.2, 3.7	SM	Task 7

Required Staffing:	14 staff months	1995
	14 staff months	1996
	14 staff months	1997
Total	42 staff months	

9.4.6 Task 6: Baseline Standards Gaps and Shortfalls for DGSA Requirements

This task requires identification and analysis of existing security standards and DGSA standards requirements to identify areas where new standards are needed and/or where existing standards require modification to be consistent with the DGSA. The first round of activities on

this task is complete. This task must be continually revisited as standards change and move forward. Continuation activities will be transitioned to a formal organization when appropriate momentum has been achieved.

Subtask 6.1: Identify DGSA Security Standards Requirements

Description: The first step of this subtask, to identify requirements from the DGSA that must result in security standards requirements, is complete. The final draft report of this activity considers the DGSA from several aspects and prescribes broad areas appropriate for standardization. The second step of this subtask, which required a documented survey of the non-Government, federal, and DoD standards, is also complete. [12] includes identification of the availability and status of current and emerging security standards. This report will require annual updates over time. The third step of this subtask requires determination of the need to develop a standards database to initially contain the survey information from step two. The database would also contain the DGSA requirements and the mapping information. Later, it would contain additional information from the standards area. The fourth step of this subtask requires development and maintenance of a database for all survey information from step two and is optional. The DGSA requirements, the mapping information, and additional information from the security standards area will be included. This step of the subtask will only be undertaken if the results of step three indicate that such a database should be developed.

Responsible Organizations: NIST: Step one. DISA CFS Steps two, three, and four.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	Prod	Task 2
	SM	Task 1		

Required Staffing:		
	21 staff months	1994
	13 staff months	1995
	11 staff months	1996
Total	45 staff months	

Subtask 6.2: Map Requirements Against Available and Emerging Standards

Description: This subtask requires the generation of a document that maps the requirements identified in the first step of Subtask 6.1 against the survey information identified in step two of Subtask 6.1. The final draft report of this activity is complete and compares the DGSA requirements to the standards survey, identifying standards that support the DGSA, as well as shortfalls and gaps. [14] will be reviewed and updated as necessary, until implementation of the complete DGSA is accomplished. A sample of the findings identified in this report are provided in Tables A-1 and A-2 in Appendix A.

Responsible Organizations: NIST

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	SM	Task 1	N/A

Required Staffing:		
	3 staff months	1994

9.4.7 Task 7: Recommendations and Guidance for Developing/Implementing DGSA Security Standards

Description: This task establishes the activities for institutionalization of the process for developing and implementing DGSA security standards. An updatable catalog of standards work

items, showing those efforts needed to overcome shortfalls and to fill gaps, will be developed. Trends (e.g., technology, policy, economics) impacting or impacted by security standards will be identified. Analysis of the results from testbeds for their impact on standards will be included. Recommendations will reflect near-term (1-4 years), mid-term (4-10 years), and long term (10 plus years) objectives. and will include identification of anticipated major events that will help to achieve the recommendations. Guidance will address issues that could hinder the development and implementation of standards, issue resolution, and the scope and functional classification of standards using the areas identified as DGSA standards requirements areas. Standards in progress will also be included in the work items. DGSA work items identified in the catalogue will be categorized and prioritized (e.g., feasibility, time frame, criticality). Necessary resources and target schedules will be identified, along with sponsorship, organizations and membership, and how the work items will be achieved. Work items that will impact DGSA transition will be highlighted.

Responsible Organizations: DISA CFS.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	Prod	Task 2
	Policy	Task 1	E&T	Task 10

Required Staffing:	16 staff months	1994
	13 staff months	1995
Total	29 staff months	

9.4.8 Resource Summary and Transition Schedule

Table 9-3 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 9-2 shows the segment transition schedule.

	Resources Required in Staff Months							
TASKS	1994	1995	1996	1997	1998	1999	2000	Total
1.1				30	30	15		75
1.2				18	18	12		48
2			22	22	22	14		80
3.1			24	36	21			81
3.2			15	15	15	12		57
3.3			20	24	18			62
4.1			24	24	14			62
4.2			24	30	14			68
4.3		33	33	32	32	32	21	183
4.4			10	16	6			32
5.1				7	8			15
5.2					6	3		9
5.3		14	14	14				42
6.1	21	13	11					45
6.2	3							3
7	16	13						29
Total	40	73	197	268	204	88	21	891

Table 9-3. Standards Segment Summary of Required Staff Resources

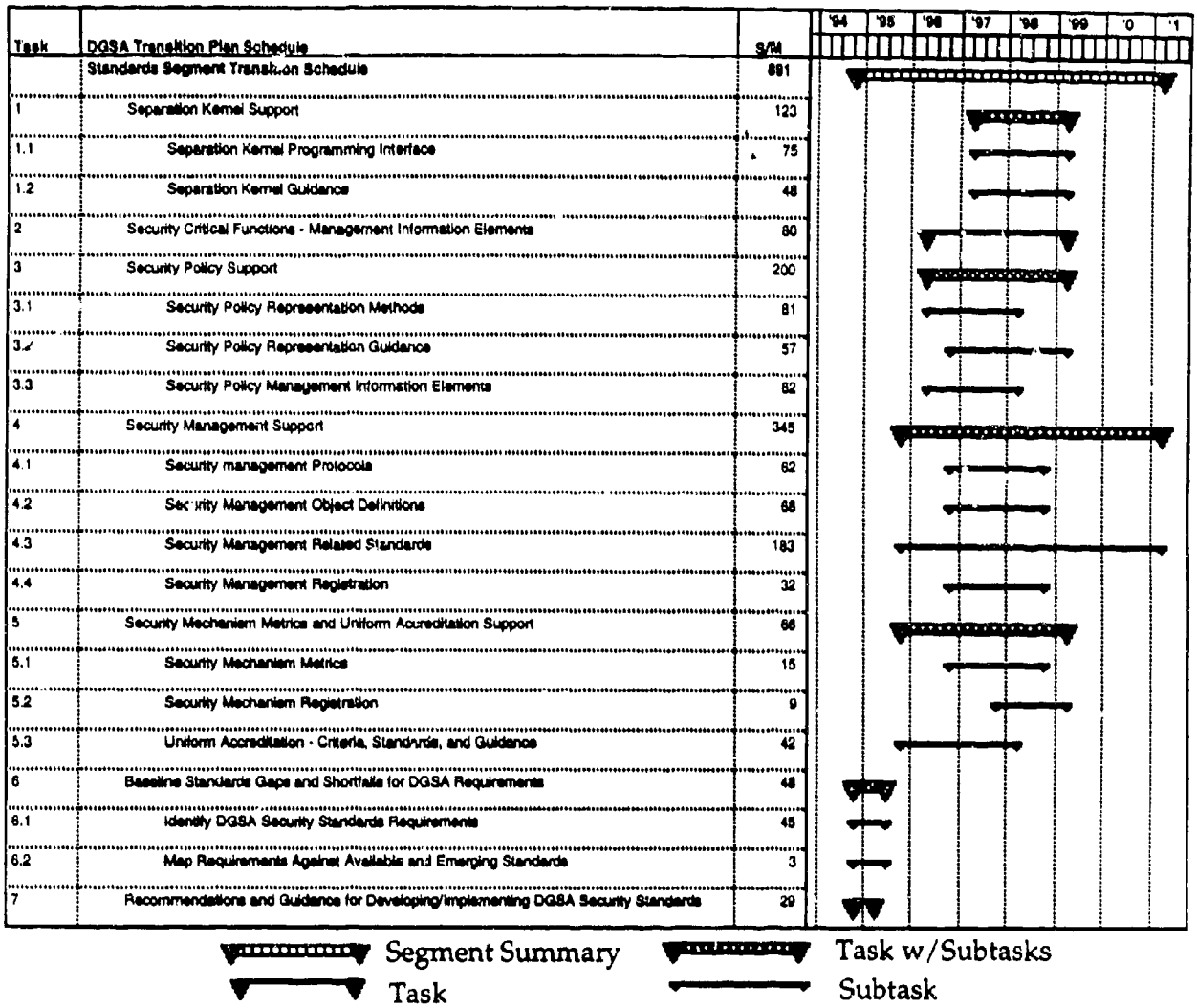


Figure 9-1 Standards Segment Transition Schedule

9.4.9 Status of Segment Tasks

Segment Accomplishments

Task 6.2 Map Requirements Against Available and Emerging Standards

The final draft report of this activity is complete and compares the DGSA requirements to the standards survey, identifying standards that support the DGSA, as well as shortfalls and gaps. *A Mapping of Standards and DGSA Standards Requirements* will be reviewed and updated as necessary, until implementation of the complete DGSA is accomplished. A sample of the findings identified in this report are provided in Tables A-1 and A-2 in Appendix A.

Segment Tasks Currently Underway

Task 6.1 Identify DGSA Security Standards Requirements

The requirements have been identified. This task must still determine whether a database for the requirements is appropriate and if so whether to implement the database.

Task 7 Recommendations and Guidance for Developing/Implementing DGSA Security Standards

This activity is ongoing and will continue until the realization of the DGSA.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 4.3 and 5.3 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

10. EDUCATION AND TRAINING SEGMENT TRANSITION STRATEGY

10.1 Introduction

The former CISS Professionalization Directorate, now part of the INFOSEC Policy, Plans, and Procedures (IP3) Directorate, developed the Education and Training (E&T) Segment in conjunction with NSA X64 in its role as National Manager for security education and training. The CISS and NSA X64 have invited participation in the (E&T) Segment Team management group by: Deputy Director IP3, CISS; the Chief, Education and Training, CISS; the Chief, Education and Training, NSA X64; the Chairman, National Security Telecommunications and Information Systems Security Committee (NSTISSC) Education and Training Working Group; and a representative from the DISA Omnibus training contractor (when selected). The E&T Segment Team members coordinate actions, as required, to facilitate introduction of the DGSA to DoD Education and Training Working Groups that currently exist or that may be organized during the transition toward the DGSA. With each working group, the E&T Segment Team establishes directed objectives for (1) Government educational institutions, (2) DoD training contractors, (3) component and agency E&T representatives, and (4) Government and industry INFOSEC leadership.

The short-term objective of the E&T Segment Team is to promote the movement of systems toward the DGSA by influencing opinion leaders and educating those that must undertake the changes. The long-term goal is to promote the adoption of DGSA principles in the E&T curricula and in the working culture, for every design, acquisition, and technical security activity in DoD. In addition to academic change, this requires a cultural shift in the manner in which information systems are built. The training objective in the DGSA is not a short-term one. The objective requires the marketing, education, and training of a large audience, over a number of years. The overall objective is to change the way people view a security architecture and how to implement concepts across it through an understanding of the DGSA and its principles.

The DGSA offers a security architecture for the DoD that, while not fully implementable today, can accommodate today's technology as part of establishing a path for future growth. In order to accomplish this feat, however, the DGSA introduces many new concepts that, in turn, will force the establishment of new ways of working with systems throughout their lifecycle. Focusing on the E&T needs of the DoD work force will ensure that qualified personnel are available to address the security of systems in the future. The E&T effort must target a very diverse audience. System architects will need to completely understand all of the concepts of the DGSA in order to use the document as guidance. Since the DGSA introduces a number of new concepts, basic security awareness courses will also need to be revised. Certifiers and accreditors will be heavily impacted by the shift to information domains and by the requirement for a life-cycle certification process. Security administrators, system developers, security evaluators and many others will also need updated E&T.

10.2 Background

The E&T Segment, like the Standards Segment, requires the development of new items and changes to existing or in process items. With respect to E&T, the process of course development or modification, course delivery, and/or course acceptance does not change with respect to the DGSA. The changes necessary are in the actual course materials and concepts being taught. The types of information security courses being offered currently, are too numerous to mention. Some examples are: general security, general computer security, general information security, network security, communications security, various physical and administrative security courses, personnel and adjudicative security, technical security countermeasures (TSCM), TEMPEST, auditing (mostly financial and operational), operating

system security, OPSEC, and preparation of security plans. Courses are also provided that cover the content of DoD 5200.28-STD. These courses are offered by both the Government and contractors. However, the majority of these courses in their current form will not educate or train the required personnel to address the DGSA concepts. The DGSA requires that fundamental notions of security being taught today be augmented by concepts such as separation mechanisms, absolute protection, strict isolation, and information domains.

In the field of security E&T, the major Government players are: (1) the NSTISSC, Education and Training Working Group, (2) the Federal Information Systems Security Educators Association (FISSEA), (3) the National Industrial Security Program, Education and Training Working Group, (4) the Joint Logistics Commanders' Information Management Panel, Education and Training Working Group, (5) the JSC, (6) NIST and (7) NSA. Industry associations such as the IEEE, Industrial Security Management Association and Information Systems Security Association also provide security E&T courses. Currently, NIST publishes a compendium of courses offered in Information Systems Security, however, this list is not verified and the courses referenced are not evaluated.

The area of security E&T has recently gained visibility due to several important events. The JSC Staff published a final report that makes recommendations in the area of professionalization for INFOSEC and Security [15]. The ASD/C3I for Information Management (IM), in response to the National Performance Review (NPR), has proposed and funded through DISA, a development effort for Information Systems Professionals which includes the Information Systems Security Career Area. The NSTISSC published the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4011 [16] in June of 1994, to describe both the content and behavioral outcomes expected of training offered in the Federal Government, for environments where classified information is processed. NSTISSI 4011, the National Training Standard for INFOSEC Professionals, is the first in a series of job-specific training standards which will follow an outline of the total array of required skill areas.

NSA and CISS are working on curricula for courses of instruction for ISSOs and Systems Administrators. The Develop a Curriculum (DACUM) for System Administrators occurred in August 1994. The result of the DACUM will be a standard curriculum for that group, published by the NSTISSC as a standard. The curriculum will need operating systems specifics, but it will be complete from the INFOSEC perspective. The NSTISSI has indicated there will be several more standards to follow. More to the point, there will be a whole series of standards that can be used to evaluate courses. Once the standards have been approved, it will be possible for NSA or CISS to evaluate courses being given by academic institutions and contractors, making training courses evaluated products.

The DISA CISS has already begun an effort to establish INFOSEC positions in Services and Agencies of DoD. No INFOSEC positions actually exist in the DoD Services or Agencies. INFOSEC personnel are part of larger career fields of computer specialists, computer scientists, engineers, and security specialists. INFOSEC positions may eventually have a description that is consistent with many career series, or alternatively, become a distinct career series. In the commercial arena, events raising the visibility of security professionalization are also occurring. For example, the National Information Infrastructure (NII) Task Force at the Department of Commerce has examined the requirements for the training of professionals who will be part of the infrastructure. Training will be an integral part of what will be funded for the infrastructure. One link to all these activities is the proposed tasking for the E&T Segment. To gain acceptance for a DGSA course, such a course will need to be framed for extremely wide audiences. To satisfy the needs of widely varied student bodies, the DGSA materials will need to be presented at a variety of levels of abstraction. In addition, many of the basic concepts will need to be taught as elementary topics in order to obtain the general understanding of a wide audience, which the DGSA requires. The major issues are: which courses to change, how to prioritize

them, what areas require new courses, and how to present the DGSA materials. The latter is perhaps the largest issue, since the E&T materials will need to draw heavily on the DGSA for course development.

A decision is needed with respect to which agency will be the Executive Agent for Training for DoD in the future. At the current time, the DoD Security Institute is interested in attaining that position. The National Cryptologic School at NSA and CISMO at CIA are also being considered for the position. It is not clear which of these organizations will eventually become the executive agent. No matter which is selected, however, it appears that the schools will be organized into a facility that provides Computer Based Training (CBT) and televised learning (similar to the PBS approach for college courses). Thus, the facility will offer consistent training and have the benefit of being "dual-use" i.e., the general population is trained on computers. The audience is also trained in information security. By strongly advertising the courses, designated audiences may be obtained. DGSA educators and trainers also need to begin to think in terms of CBT and televised learning.

10.3 Transition Approach

The E&T Segment works through the DISA CISS P3I Directorate to obtain access to several organizations that are currently engaged in curricula development. The NSA/NIST DACUM Working Group, is funded by NSA and jointly sponsored by NIST. Its membership is drawn from all parts of the federal Government. The E&T Segment also has access to the Curriculum Development Working Group of the Defense Security Institute. Finally, the E&T Segment has access to the Curriculum Panel of the Defense Acquisition Management College. It is necessary to approach each of these working groups with the objective of having the DGSA presented to faculty members and non-instructor curriculum developers. Specific audiences for courses are clearly identified and curricula for each audience are established and tailored, as necessary. Once developed, a curriculum is usually passed through the Education and Training Working Group of the NSTISSC and the NIST Education and Training Working Group, as well as the FISSEA. If sanctioned by all three groups, the curriculum is generally acceptable to E&T specialists in the Government INFOSEC community.

After coordination of the curriculum with the E&T groups noted, a harmonized curriculum suitable for DoD is developed.

1. Established curricula are harmonized and further distributed to other institutions as modules.

2. Initial placement of modules is undertaken, most likely in Government facilities.

3. DGSA principles and training objectives are presented for industry E&T.[1]

4. Educational and/or training courses and materials are expanded for at least eight audience categories within the DoD establishment: (1) executives, (2) managers with Designated Approving Authority (DAA) responsibilities, (3) managers with systems responsibilities, including Information Resource Management (IRM), (4) acquisitions or program managers, (5) system administrators, (6) hardware and software developers, including architects and engineers, (7) vendors, and (8) systems and network security officers.

[1] The organization most responsible for industry training is the National Industrial Security Program, Education and Training Working Group.

While E&T activities are being pursued, marketing initiatives must also be underway. Marketing efforts are designed to create an awareness of the existence and importance of the DGSA through executive-level briefings and the publication of conceptual papers. The E&T Segment Team may be involved in the development of marketing materials for the DGSA and in the actual delivery of DGSA presentations. The recognition of importance provided by DGSA marketing must be followed up with education and, where appropriate, training with respect to implementation.

The E&T approach recommended, addresses the needs of the complete work force. Security awareness and training courses for all personnel will be updated to reflect the more balanced perspective of doctrine offered by the DGSA. Security management courses will be developed to train security administrators in the proper initialization of systems to support mission-specific policies as well as all other job functions routinely undertaken. Security architects will be well versed in the intricacies of system interconnection and support for multiple information domains. System certifiers and accreditors will be called in during the early stages of development. Certifiers and accreditors will understand the need for their active involvement in the system development lifecycle, from the Mission Need Statement through the routine re-accreditation process.

There are three major transition points for E&T. The first will occur in FY 1995. The development of marketing materials should be complete and the marketing program should be in-process. At this point, the DGSA should have been thoroughly advertised through the publication of short conceptual papers which will be presented at symposiums and conferences.

The second transition point for E&T will occur in FY 1997, with the completion of the development and modification of all basic courses. An educational and motivational course should be completely developed and the security awareness courses appropriately modified. The NSA cryptologic school courses shall have been modified. A new INFOSEC management course should be completely developed. Such courses should have already been experimented with in the classroom so that positive results are assured. In addition, all major courses will have been modified to accommodate the DGSA. Revisions to the OPSEC courses will be complete. The architect and engineering trainers will have modified their courses. The security administration training and education course modifications will be complete. Likewise, both the C&A process education course and the training course will be complete. Courses for teaching the trainers will also be complete, with some trainers already prepared and others in the training pipeline to receive training.

The final transition point for E&T will occur in fiscal year 1998. By then, the courses supporting transition to the DGSA should largely be institutionalized. All curricula will have been modified to incorporate any new courses developed in support of the DGSA. The activities for maintaining and teaching the courses over time will have been transitioned to their parent organizations. Security themes related to the goal architecture will be a standard way of educating and training new personnel.

10.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being

described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 10.4.13. Subsection 10.4.14 provides the status of each segment task.

10.4.1 Task 1: DGSA/Transition Marketing

The purpose of this task is to prepare materials for the purpose of marketing the DGSA and DOTS. Such materials will include an executive briefing, brochure, and a videotape.

Subtask 1.1: Executive Brief

Description: An executive briefing will be prepared to provide a summary and overview of the DGSA concepts, using graphics, video, and voice to illustrate examples. The briefing will contain a summary of concepts with advantages and disadvantages clearly stated. The informational content will include closing actions required of the viewer. A three member team will be provided to present the briefing.

Responsible Organization: DGSA Core Team

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
Required Staffing:	3 staff months	1995	
Total	3 staff months		

Subtask 1.2: High Level Managers Handouts

Description: This subtask requires the development of handouts to accompany the high level executive briefing. The handouts may include a summary sheet, fact sheet, brochure, and copy of the brief on diskettes (compressed).

Responsible Organization: Primary: DISA CISS. Support: DGSA Transition Team manager.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
Required Staffing:	2 staff months	1995	

Subtask 1.3: Videotape Preparation

Description: This subtask requires development of a 15 minute motivational summary of the DGSA concepts as they apply to a DoD Program Manager. The presentation will summarize major concepts highlighting advantages to the Government and to the individual manager for using the approach. The presentation closing will give a point of contact for additional information and encourage additional involvement.

Responsible Organization: Primary: DISA CISS. Support: DGSA Transition Team manager.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	

Required Staffing: 5 staff months 1995

10.4.2 Task 2: Educational / Motivational Course

Description: This task requires development of a one-day educational and motivational follow-up course at the graduate or undergraduate level. The course will provide a short summary and review of major DGSA-related concepts, and practical applications within a seminar session. The learning objective is to apply the principles of the DGSA to procurements. A two-person team will be provided to present the course.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	

Required Staffing:	3 staff months	1995
	3 staff months	1996
Total	6 staff months	

10.4.3 Task 3: Modify Courses to Accommodate DGSA

This task requires, either directly or indirectly, supporting the development of modifications to existing courses to include material on the DGSA. The best approach to presenting the DGSA materials will be determined.

Subtask 3.1: Modify NSA Cryptologic School Courses

Description: This subtask requires modification of the NSA Cryptologic School courses that are under existing contracts. Such modifications will permit new materials to be assessed by a group of students and teachers that have consistent backgrounds. Thus new materials can be revised, if necessary, prior to a broad introduction of new course materials.

Responsible Organization: NSA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,8	
	LSE	Tasks 3,5	
	CN	Subtasks 3.1,3.2,4.3	

Required Staffing:	3 staff months	1995
	2 staff months	1996
Total	5 staff months.	

Subtask 3.2: Delivery Methods Study

Description: This subtask requires a study of the best delivery methods for new security course materials. The study will include an examination of the current DoD use of remote delivery methods and the adaptability of course materials to the existing technologies. The study will provide a cost analysis of the optimal cost/benefit methods of course delivery that includes one-time start-up costs and continuing costs over a 5 year period.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
Required Staffing:	2 staff months	1995	

Subtask 3.3: Assist Architecture and Engineering Trainers with Courses

Description: This subtask requires that assistance be provided to the architecture and engineering trainers and educators for the development of materials for use in graduate level courses.

Responsible Organization: DISA CISS, A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
	LSE	Tasks 3,5,7	
	CN	Subtask 3.1	
Required Staffing:	1 staff month	1996	
	1 staff months	1997	
Total	2 staff months		

10.4.4 Task 4: Modify Curricula

Description: This task requires DGSA-related modifications of security awareness course materials to an appropriate reading and comprehension level for distribution to Security Awareness Programs at installation and station levels.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
Required Staffing:	1 of a staff month	1997	
	1 of a staff month	1998	
Total	2 staff month.		

10.4.5 Task 5: Influence Existing Security Awareness Courses

Description: This task requires the development and distribution of supporting materials and handouts for the modifications prepared in Task 4. Such materials will be provided at installation and station levels to update the existing Security Awareness Course(s).

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Tasks 1,10	

Required Staffing:	1 staff month	1995
	1 staff month	1996
	1 staff month	1997
Total	3 staff months	

10.4.6 Task 6: Revisions to OPSEC Courses

Description: This task requires revisions to existing OPSEC courses to describe the nature of threats in a DGSA-based environment, and modifications of LSEs required to support the DGSA.

Responsible Organization: NSA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	LSE	Task 8
	SM	Task 1		

Required Staffing:	1 staff month	1995
	2 staff months	1996
Total	3 staff months	

10.4.7 Task 7: Management and Administration Courses

The DGSA will promote significant changes in the area of security management and administration. Thus, new education courses will be necessary in both areas. In addition, training courses will be required to ensure that security administrators have the requisite skill sets to perform their required functions.

Subtask 7.1: INFOSEC Management Course

Description: This subtask requires development of a one day INFOSEC Management Education Course. This course is intended to provide an overview of all security management aspects of systems that are DGSA-consistent.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	N/A	
	SM	Tasks 1,8,12		

Required Staffing:	3 staff months	1995

Subtask 7.2: Security Administration Training and Education Course

Description: This subtask requires development of a two-week security administration training and education course. The purpose of this course is to educate INFOSEC professionals in security administration of LSEs and the infrastructure systems and to train them on techniques to audit and administer security in the new systems that are DGSA-consistent.

Responsible Organization: Primary: DISA, Support: DISA CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	Policy	Task 1	N/A	
	SM	Tasks 1,8,11,12		

Required Staffing:	10 staff months	1995
	20 staff months	1996
	6 staff months	1997
Total	36 staff months	

10.4.8 Task 8: Train the Training Deliverers

Description: This task requires development of a 5 day comprehensive course that will provide all necessary information for institutions and corporations that currently provide commercial educational and training courses.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	

Required Staffing:	9 staff months	1996
	4 staff months	1997
	2 staff months	1998
Total	15 staff months	

10.4.9 Task 9: Certification and Accreditation (C&A) Courses

This task requires the development of new C&A education and training courses. These courses will reflect the new C&A process developed by the C&A Segment for DGSA transition.

Subtask 9.1: C&A Process Education Course

Description: This subtask requires development of a new C&A Basic Issues Course for INFOSEC certifiers and accreditors. This course will be a supplemental course for C&A professionals enrolled in individual certification (certificate acquisition) programs.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
	C&A	Task 4	

Required Staffing:	8 staff months	1996

Subtask 9.2: C&A Process Training Course

Description: This subtask requires development of a C&A Process Training Course for INFOSEC certifiers and accreditors. This course will ensure that certifiers and accreditors have the basic skills necessary to assess systems that are DGSA-consistent.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	
	C&A	Task 4	

Required Staffing:	6 staff months	1996
	13 staff months	1997
Total	19 staff months	

10.4.10 Task 10: Policy and Standards Education Courses

Description: This task requires the development of a Policy and Standards Overview Course. This educational course will provide support for many different cross-functional skill levels and career fields. This course will address the principle security policies and standards, with a focus on changes resulting from adoption of the DGSA.

Responsible Organization: DISA.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Tasks 1 through 4	N/A
	SM	Task 1	
	STD	Tasks 2,3,5, Subtasks 1.1, 4.1, 4.3,4.4,6.1	

Required Staffing:	4 staff months	1996
	4 staff months	1997
Total	8 staff months	

10.4.11 Task 11: Publish Short Conceptual Papers

Description: This task requires writing, presentation, and publication of brief (10 page) conceptual papers. Such papers will illustrate the basic concepts of the DGSA and their foundations. Publication may occur via the various professional conferences.

Responsible Organization: DISA CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	

Required Staffing:	7 staff months	1995

10.4.12 Task 12: DGSA Advanced Architecture Level Course

Description: This task requires the development of a DGSA graduate-level course for seniors of the INFOSEC profession. This course will describe the details of the DGSA in sufficient detail to allow a college graduate student to apply the DGSA principles in other courses in network or communications design, open systems architectures, client-server systems, and multi-use globally interconnected infrastructure development.

Responsible Organization: DISA CISS A&E Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	Policy	Task 1	N/A
	SM	Task 1	

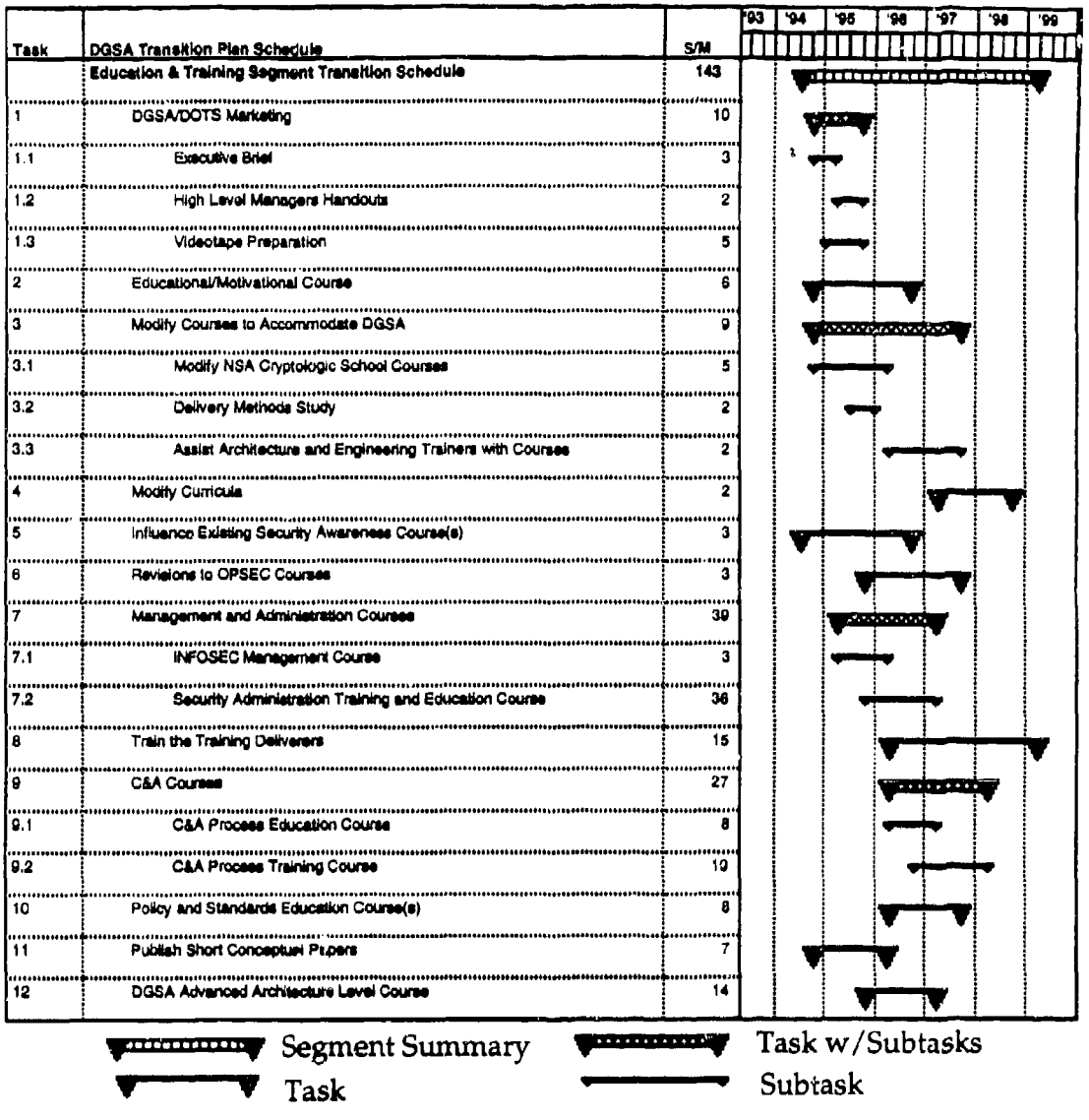
Required Staffing:	5 staff months	1995
	9 staff months	1996
Total	14 staff months.	

10.4.13 Resource Summary and Transition Schedule

Table 10-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 10-1 shows the segment transition schedule.

	Resources Required in Staff Months				
Task	1995	1996	1997	1998	Total
1.1	3				3
1.2	2				2
1.3	5				5
2	3	3			6
3.1	3	2			5
3.2	2				2
3.3		1	1		2
4			1	1	2
5	1	1	1		3
6	1	2			3
7.1	3				3
7.2	10	20	6		36
8		9	4	2	15
9.1		8			8
9.2		6	13		19
10		4	4		8
11	7				7
12	5	9			14
Total	45	65	30	3	143

Table 10-1. E&T Segment Summary of Required Staff Resources



Task	DGSA Transition Plan Schedule	S/M
	Education & Training Segment Transition Schedule	143
1	DGSA/DOTS Marketing	10
1.1	Executive Brief	3
1.2	High Level Managers Handouts	2
1.3	Videotape Preparation	5
2	Educational/Motivational Course	6
3	Modify Courses to Accommodate DGSA	9
3.1	Modify NSA Cryptologic School Courses	5
3.2	Delivery Methods Study	2
3.3	Assist Architecture and Engineering Trainers with Courses	2
4	Modify Curricula	2
5	Influence Existing Security Awareness Course(s)	3
6	Revisions to OPSEC Courses	3
7	Management and Administration Courses	39
7.1	INFOSEC Management Course	3
7.2	Security Administration Training and Education Course	36
8	Train the Training Deliverers	15
9	C&A Courses	27
9.1	C&A Process Education Course	8
9.2	C&A Process Training Course	19
10	Policy and Standards Education Course(s)	8
11	Publish Short Conceptual Papers	7
12	DGSA Advanced Architecture Level Course	14

Figure 10-1 Education and Training Segment Transition Schedule

10.4.14 Status of Segment Tasks

Segment Accomplishments

None of the segment tasks have been completed.

Segment Tasks Currently Underway

Task 1.1 Executive Brief

This task is being undertaken by the DGSA Core Team and should be completed in 2QFY95.

Task 1.2 High Level Managers Handouts

This task is being undertaken by the DGSA Core Team and should be completed in 2QFY95.

Task 11 Publish Short Conceptual Papers

This task is being undertaken by the DGSA Core Team. Initial papers should be available in FY95.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 1.3, 2, 3.1, 3.2, 5, 6, 7.1, 7.2, and 12 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

(This page is intentionally blank.)

11. CERTIFICATION & ACCREDITATION SEGMENT TRANSITION STRATEGY

11.1 Introduction

This transition strategy addresses the concerns for the C&A area with respect to transitioning toward the DGSA Appropriate C&A planning is critical to the overall success of attaining the DGSA. As the future security vision for DoD information systems is established by the phased implementation of the DGSA, a comprehensive evaluation of the technical and non-technical security features will be required. The comprehensive evaluation, referred to as security certification, is made in support of the accreditation process. Security certification establishes the extent to which a particular design and implementation meet a set of specified security requirements. Today's C&A policy and methods are too costly and complex to be applied to the emerging information system infrastructure. The C&A segment focuses on the processes for assessing the effectiveness of system security implementation in fielded systems and for approving the operation of systems. The C&A segment leader is provided under the auspices of the Directorate, CISS.

The specific goals of the C&A segment, based on the DGSA recommendations and goals, are:

- Develop/identify a new process for C&A that supports the DGSA and addresses threats and risk management.
- Ensure C&A is a measurable activity that permits enforcement of the DGSA recommendation for consistency.
- Provide an approach for gaining acceptance and approval for the new C&A paradigms.
- Ensure the results of the new C&A process will be reusable.
- Assist in the development of new C&A training materials.
- Ensure any new C&A policies include identification of responsibilities and methodology descriptions.

The C&A segment will adhere to the objectives of cost reduction, efficiency, interoperability, and consistent security. A strategy that shows long-term benefits and reductions in cost, typified by the reuse of C&A results and a reasonable approach to recertification of systems and products after changes, is strongly recommended.

Security mechanisms of information systems will be evaluated in terms of their ability to support information domain security policies. New C&A processes will ensure that the results of security mechanism C&A are reusable for part or all of one or more missions. Given the needs for sharing and separation, the C&A procedures will need to be consistent, uniform, and applicable across DoD systems and products. The C&A transition recognizes, and requires investigation of, the role of security certification as part of the system engineering process. The establishment of a standard C&A process will:

- Standardize security activities (eliminating redundancy and gaining uniformity) and associated documentation.

- Identify levels of certification analysis for each security information domain.
- Be applicable to any type of acquisition strategy or development.
- Be applicable regardless of system lifecycle stage and provide immediate feedback.
- Remain constant whether the assets are allocated to an end system with multiple information domains, a relay system, or the Local Communication System.
- Promote economy of resources through reuse of previous solutions, decisions and resources, by elimination of excessive documentation, and through encouraging the use of evaluated products.
- Eliminate confusion caused by inconsistent regulations and processes, and inexperienced certification teams.

The C&A segment leverages off of the Security Process Improvement Working Group (SPIWG) which was formed in response to tasking outlined in Office of Assistant Secretary of Defense (OASD) Memorandum, "The Defense Information Systems Security Program Strategic Plan," August 1992. The memo tasked the DISSP with the creation of standardized requirements and processes for the accreditation of computers, systems, and networks. The SPIWG consists of members from the Services and many DoD Agencies. Leveraging off of the SPIWG efforts is logical since its goals are nearly identical to the goals of the DOTS C&A transition segment and thus, duplication of efforts is prevented. The SPIWG is chartered by a recognized authority and is funded. The SPIWG is active with on-going C&A activities and has a deliverable that will become the DoD standard.

11.2 Background

Although DoD 5200.28 mandates the C&A of all systems, the interpretation and implementation of this policy varies widely [17]. Currently many systems go unaccredited since there are not enough qualified certifiers and there is much divergence of opinion with regard to the specifics of the C&A process [18]. The current C&A process is essentially ad hoc, undertaken on a system-by-system basis with no uniformity or standardization. To achieve an integrated, cost-effective security program within DoD, a standard process that can be uniformly applied must be developed [19].

Existing and draft guidance is typically directed at the acquisition of a major computer system [20] and does not meet the user needs for C&A at any time in the life cycle. This guidance is not flexible or adaptable and does not recognize that certification can be performed at various levels of abstraction or technical depth. The OASD Memo [the strategic plan], tasked the DISSP with creating a standardized set of requirements and a process for accreditation [17]. In February of 1993, the OASD for C3I requested that the CISS provide an analysis of the security C&A process with the objective of formulating a standard C&A process [17]. The OASD C3I established a high-level Security Process Improvement Steering Group under the Chairmanship of the CISS. This steering group in turn established the SPIWG, under the DISSP auspices.

The working group undertook the analyses of eight different C&A processes [21], ranging from military to academic to civilian systems. The results of those analyses showed that all of the eight processes were based on defining requirements, conducting a risk analysis, and using a life cycle management approach [21]. The SPIWG was also tasked with the development of a framework for a C&A process [22] with the following four characteristics: 1) quantitative, 2) tailorable, 3) scaleable, and 4) predictable. The eventual process drafted was called the DoD

Information Technology Security Certification and Accreditation Process (DITSCAP), which continues to be under development. The process defined in the DITSCAP contains four steps that are applicable to every system. These steps will vary in the amount of activity and depth of detail as they are tailored and scaled for a specific system and its residual risk.

During the same time frame, the National Computer Security Center (NCSC) had been working on a guideline for C&A. This guideline was published as *Introduction to Certification and Accreditation*, NCSC-TG-029, Version 1 [19], in January 1994. Earlier, in May of 1993, the NCSC released a draft of the Certification and Accreditation Process Handbook [23]. This handbook establishes a standard approach for performing C&A, provides guidance on the level of effort required to satisfy various assurance requirements, and provides other tailoring factors [23]. The draft DITSCAP and the draft C&A Process Handbook have currently been undergoing a harmonization effort. A coordination draft of the harmonized version of the DITSCAP was released in July 1994.

11.3 Transition Approach

The C&A segment for transition will employ the results of all other segment teams to determine compliance with policy. The C&A segment is essentially dependent on all other segments within the DGSA transition process. As a result, the success of applying a new C&A process for the DGSA will be a measure of how well all segments within the transition process are integrated. The issues that are encountered by certifiers and accreditors during implementation will reflect any shortcomings in the transition approaches of all segments. The overall approach to transition for the C&A segment is summarized in the steps listed below.

- Develop a thorough understanding, through analysis, of how evaluation and C&A are currently undertaken, documenting the results as a short study.
- Outline the DGSA principles that impact the C&A process.
- Identify the C&A requirements that meet the DGSA needs.
- Develop a schedule and milestones to implement the new evaluation and C&A process.
- Identify new activities required in support of the new process and support the education and training segment in the development of training materials for these activities.
- Foster the development of tools and procedures that will support the new C&A process and promote the establishment of metrics for the new process.

There are three major transition points for C&A. The first will occur in fiscal year 1995. At this point, all C&A requirements should have been identified. This includes, not only the DGSA related requirements, but all functional requirements as well. Also by the end of 1995, the new C&A process should be completely defined. Along with the process, any requirements for metrics and any process dependencies should be identified, the security management functions for users and security managers should be defined, and any additional activities in support of the new process should be outlined. Finally, a new accreditation policy should be in place that supports and requires the new C&A process and DISSP-SP.1 to have final approval so that all DGSA related aspects of the new C&A process can move forward.

The second major transition point for C&A will occur in FY 1997. At this point, any new metrics and profiling techniques required should be fully defined and tested and the development

of a mechanism catalog and the metrics should be underway. The new uniform C&A process should be fully documented, widely distributed, and in field use. This documentation should be in use for the development of associated uniform C&A standards, criteria, and guidance. The marketing efforts for the new C&A process should be in full swing. Finally, education and training courses based on the new C&A process should be in place.

The final major transition point for C&A will occur in FY 1999. At this point, it is anticipated that all major revisions to the DGSA that could have an impact on C&A will be complete. Guidelines for addressing both local and distributed SM that include the allocation of associated responsibilities, will be complete. The new C&A related metrics and profiling techniques will be in place and will be used consistently. This will be due in part to the fact that the uniform accreditation standards, criteria, and guidance will be complete and in general use. The marketing efforts to obtain buy-in for the new C&A process and its associated activities will be complete. Finally, C&A E&T courses will be a normal part of accepted curriculums.

11.4 Segment Transition Tasks

The following sections define the tasks needed to achieve the Policy Segment goals required by the DGSA. For each task or subtask, the following information is provided: (1) a general task description, (2) identification of responsible organization, (3) staffing resources required, and (4) inter-task dependencies. Tasks listed in the Inter-task dependencies section are identified as either Input Dependencies or Output Dependencies. Input Dependencies are those tasks that are producing something required to complete the task being described. Output Dependencies are those tasks whose completion is dependent on completion of the task being described. Some of the resources required to carry out these tasks are part of existing activities. These activities are included as part of this segment strategy. A resource summary and transition schedule for the segment is presented in Subsection 11.4.6. Subsection 11.4.7 provides the status of each segment task.

11.4.1 Task 1: Identify/Analyze/Document Current C&A Process

Description: The purpose of this task was to define the current C&A process by gathering information from the MILDEPs and accreditors. The output of this task was a definition of the current process and results of analysis identifying what is acceptable, what needs to be fixed, and what needs to be added to improve the process. To achieve DoD-wide consensus on this subject, the DoD Security Accreditation Working Group (DSAWG) was the forum in which this topic was discussed, recommendations were reviewed, and issues were resolved or tabled.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: MILDEPS, major [illegible] representatives, and NSA C and I9.

Inter-Task Dependencies:	Input Dependencies	Output Dependencies
	SM Task 1	N/A

Required Staffing: 8 staff months 1994

11.4.2 Task 2: DGSA Principles & Requirements Impacting C&A

This task is comprised of two subtasks related to defining specific DGSA principles and derived requirements which impact the new C&A process to be developed. These subtasks are critical to a coordinated transition toward the DGSA target. This task includes a C&A strategy for Product and LSE technical evaluation which is in consonance with INFOSEC product evolution and migration, and includes transition milestones for migrating toward a new division of accreditation responsibilities (domain/mission/enterprise). Organizational responsibilities, staffing, and links to other segments are described for each subtask.

Subtask 2.1: DGSA Principles Impacting C&A

Description: The purpose of this subtask is to identify DGSA principles which directly apply to, and impact C&A process activities. This includes adopting the concept of information domains, and ensuring the principles of security contexts and associations, SM, strict isolation, absolute protection, and uniform accreditation are instilled into the C&A process. On-going discussions between the C&A segment, the Evaluation, Certification and Accreditation (EC&A) Directorate, and the DGSA architects, will ensure the C&A process includes the DGSA principles. The results of this activity will be inputs to Tasks 3, 4, and 5. The results of this subtask will also become inputs to the SM, Policy, Product Development, R&T, and Standards segments tasks. Although no specific tasks have been identified to date, correlation with other segment tasks is critical at some point.

Responsible Organization: Primary: DISA CFSE. Support: DISA CISS EC&A Directorate.

Inter-task Dependencies:	Input Dependencies SM Task 1		Output Dependencies N/A
Required Staffing:	6 staff months	1994	

Subtask 2.2: Identify C&A Requirements From DGSA

Description: The purpose of this subtask is to identify and describe the specific C&A requirements explicitly and implicitly derived from the DGSA. These requirements are anticipated to include such elements as: content definition for information domain security policies; strict isolation metrics and migration guidance; absolute protection criteria; uniform accreditation guidelines; design guidance for supporting multidomain objects; and interdependency analysis guidelines.

Responsible Organization: DISA CFSE.

Inter-task Dependencies:	Input Dependencies SM Task 1		Output Dependencies N/A
Required Staffing:	60 staff months	1994	

11.4.3 Task 3: New C&A Process Development & Documentation

The purpose of this task is to develop, document, market, and gain DoD-wide concurrence for a new C&A process. The new process will reflect the principles and requirements of the DGSA. The task is composed of the seven subtasks (11.3.1 - 11.3.7) described below. Organizational responsibilities, staffing, and links to other segments are described for each subtask.

Subtask 3.1: Develop New C&A Process

Description: The purpose of this subtask is to amend any problems identified, with respect to the current C&A process, and ensure that the new C&A process includes the requirements from the DGSA. That is, this subtask ensures that the results of Tasks 1 and 2 are incorporated into the new C&A process. Intermittent reviews of the new process with each of the other segment areas should be undertaken to ensure harmony throughout the transition process.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CFSE (The DSAWG members will participate intermittently in order to gain consensus for the new process as it develops).

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	Policy	Task 4
	Policy	Task 1	STD	Subtask 5.3

Required Staffing:		
	96 staff months	1994
	96 staff months	1995
Total	192 staff months	

Subtask 3.2: Identify Responsibilities for New C&A Process

Description: The purpose of this subtask is to define the approach for providing independent, unbiased certification organizations and to define their responsibilities. In addition, this subtask will delineate the approving authorities and the responsibilities of each organization. The accreditors will range from owners/caretakers of specific information (information domain accreditors) to the oversight bodies of mission and enterprise accreditors. The results of C&A Task 2 will be used by this subtask.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CFSE, mission area representatives, and NSA C.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	STD	Subtask 5.3
	Policy	Task 1		

Required Staffing:		
	54 staff months	1995

Subtask 3.3: Define C&A Metrics & Other Process Dependencies

Description: The purpose of this subtask is to define how metrics are used throughout the system security engineering process. Additionally, this subtask will define how the metrics and other methods (e.g., interdependency analysis), and output from system profiling activities assist in, and are integrally part of, the new C&A process.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CFSE, mission area representatives, NSA C, and NSA system profiling organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	SM	Tasks 7,11,12
	Policy	Task 1	STD	Subtask 5.3

Required Staffing:		
	99 staff months	1994
	33 staff months	1995
Total	132 staff months	

Subtask 3.4: Define Acceptance Approach for New C&A Process

Description: The purpose of this subtask is to develop a marketing approach to sell the new C&A process to the enterprise and all of the DoD mission areas.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DSAWG members.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	SM	Task 1	N/A
	Policy	Task 1	

Required Staffing:	6 staff months	1994
	6 staff months	1995
Total	12 staff months	

Subtask 3.5: Market New C&A Process (Gain Concurrence)

Description: This subtask exercises the acceptance approach/marketing strategy developed in Subtask 3.4 by briefing each of the mission areas and OSD and selling the benefits of the new C&A process. The subtask includes employing the members of the DSAWG to sell the new process to those organizations each DSAWG member represents. This is the implementation of the approach for establishing the new C&A process and overseeing it to ensure it is working correctly throughout DoD.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DSAWG members.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	SM	Task 1	N/A
	Policy	Task 1	

Required Staffing:	24 staff months	1996
	36 staff months	1997
	36 staff months	1998
Total	96 staff months	

Subtask 3.6: Identify Additional Activities for New Process

Description: The purpose of this subtask is to identify, define, and include any additional activities which must be incorporated in the new C&A process, or which are needed to support the new C&A process.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CFSE, mission area representatives, NSA C, and NSA system profiling organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies
	SM	Task 1	N/A
	Policy	Task 1	

Required Staffing:	78 staff months	1995

Subtask 3.7: Document Uniform C&A Processes

Description: The purpose of this subtask is to develop the guidance documentation for uniform C&A processes. This subtask will be implemented in parallel with all Task 3 subtasks.

Responsible Organization: DISA CISS EC&A Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	STD	Subtask 5.3
	Policy	Task 1		
Required Staffing:	9 staff months	1994		
	15 staff months	1995		
	6 staff months	1996		
Total	30 staff months			

11.4.4 Task 4: Coordination for Development of C&A Training Materials

Description: The purpose of this task is to define and coordinate training materials and training approaches to teach the new C&A process to all functional elements of each mission area. This will be performed in cooperation with the DISA CISS Professionalization Directorate.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CISS Professionalization Directorate.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Task 1	E&T	Subtasks 11.1,11.2
	Policy	Task 1		
Required Staffing:	24 staff months	1994		
	24 staff months	1995		
Total	48 staff months			

11.4.5 Task 5: Apply New Metrics and Profiling

Description: The purpose of this task is to include the usage of new metrics, and product and system profiling documentation in the C&A documentation. Only metrics and documentation that have gained a consensus for their use and usefulness as applied to the C&A process will be included. This task is also a coordination and joint development task; i.e., CISS EC&A and NSA C organizations working with the NSA product and system profiling organizations to ensure a consensus on how metrics and profiling are being developed and matured can assist and support the C&A process. When and if consensus is reached, the consensus perspective will be included in the uniform C&A documents.

Responsible Organization: Primary: DISA CISS EC&A Directorate. Support: DISA CFSE, mission area representatives, NSA C, and NSA profiling organizations.

Inter-task Dependencies:	Input Dependencies		Output Dependencies	
	SM	Tasks 1,7,12	N/A	
	Policy	Task 1		
Required Staffing:	39 staff months	1996		
	78 staff months	1997		
Total	117 staff months			

11.4.6 Resource Summary and Transition Schedule

Table 11-1 contains a summary of the required resources to complete the tasking outlined in this segment strategy by fiscal year. Figure 11-1 shows the segment transition schedule.

	Resources Required in Staff Months					
Task	1994	1995	1996	1997	1998	Total
1	8					8
2.1	6					6
2.2	60					60
3.1	96	96				192
3.2		54				54
3.3	99	33				132
3.4	6	6				12
3.5			24	36	36	96
3.6		78				78
3.7	9	15	6			30
4	24	24				48
5			39	78		117
Total	308	306	69	114	36	833

Table 11-1. C&A Segment Summary of Required Staff Resources

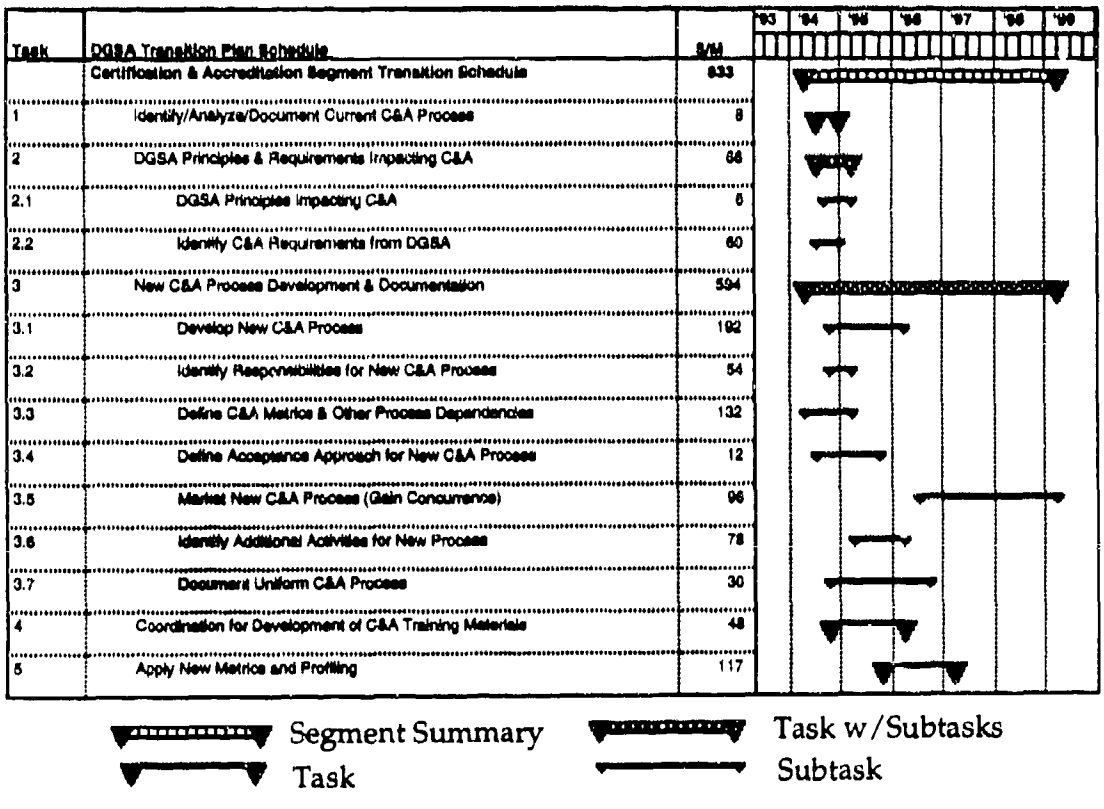


Figure 11-1 Certification and Accreditation Transition Schedule

11.4.7 Status of Segment Tasks

Segment Accomplishments

Task 1 is complete.

Segment Tasks Currently Underway

Task 2.1 DGSA Principles Impacting C&A

This task is underway.

Task 2.2 Identify C&A Requirements from DGSA

This task is underway.

Segment Tasks Not Being Performed

The organizations assigned to Tasks 3.1, 3.2, 3.3, 3.4, 3.6, 3.7, and 4 have not assumed responsibility for the tasks, therefore these tasks have not started as scheduled.

APPENDIX A REPRESENTATIVE PRODUCTS SUMMARY

This appendix to the DOTS products work plan summarizes INFOSEC products in the following ways:

- Those products which are currently available
- Those products which are in the evaluation/certification pipeline
- Those products which are currently under development
- Those products which are planned to be under development (e.g., future MISSI Releases which do not yet have a finalized schedule)
- Product concepts being explored in research and technology (e.g., enhanced separation technology, security management mechanisms, biometric mechanisms)
- Product concepts that need exploration but are not yet formally in the R&T pipeline (i.e., many of the items mentioned in the DOTS R&T work plan)
- Products which are likely to result from current standards work (e.g., IEEE KMP, ISO GULS, etc.)
- Products which are in development or planned development that conflict with current standards work, and which will significantly constrain interoperability with future products; i.e., those that will follow the new standard(s). An example is the SAMP developed by Motorola for the STE. This protocol is incompatible with the IEEE Key Management Protocol (KMP) which is also a generalized security association management protocol that will end up as an international standard.

The products summary included here is a representative view; it does not include all INFOSEC products. The populated products database will include all INFOSEC products.

INFOSEC PRODUCTS *CURRENTLY AVAILABLE*

-- A Representative View

PRODUCT CATEGORY	GENERAL DESCRIPTION
I. WORKSTATIONS &WS - SIZE HOSTS AND SERVERS -- can be used as Guards and Secure Relay Systems	All of the secure workstations are UNIX based -- some have a DOS emulation mode. General problem with all of the representative workstations is that they do not incorporate network security features, there are no standard security management features and they can not support multiple simultaneous security policies. They can, however, be made to support multiple information domains, but the isolation of domains is at the low end (B1) & low/med end(B2) level of strength. They do fit into the DGSA transition, but only as near- to mid-term transition components.
Harris CX/SX	TCSEC class B1 workstation (UNIX)
Hewlett-Packard HP-UX BLS	TCSEC class B1 workstation (UNIX)
SecureWare CMW+ (a/ux)	TCSEC class B1 & CMW B1+ (Macintosh version of System 3 UNIX)
UNISYS OS 1100/2200	TCSEC class B1 (proprietary operating system for C-series instruction processors)
DEC SEVMS	TCSEC class B1 (DEC proprietary operating system - claims POSIX compliance
AT&T System V/MLS	TCSEC class B1 (System V UNIX is as close to POSIX as one can come)
TIS Trusted Xenix 3.0	TCSEC class B2 (System 3 UNIX) for IBM PC/AT, PS/2 or PC/AT clones (intel 286/386/486 based)
II. Hosts	Hosts have traditionally been viewed as mini and mainframe devices. With the increase in micro processing power, upper end memory capability and I/O speeds, however, micros (those identified above as workstations) can, and are, also considered hosts when they support multiple simultaneous users connect to a network. The philosophy of "Mega Data Centers" being pursued by DISA CFA & CFII organizations, when synergized with distributed workstation/server technology, could put new life expectancy into the DoD mainframe market and cause mainframes to be around for many years to come.
IBM MVS/ESA	TCSEC class B1 for IBM 3090 and IBM 4381 mainframes-- first of the mainframe operating systems to achieve this low end level of isolation assurance. Evaluation based on VM/SP 3.1 operating system and RACF 1.9
Amdahl UTS/MLS	TCSEC class B1 - mainframe
Cray UNICOS 8.0	TCSEC TNI class B1 -- mainframe. MLS version of general purpose OS based on UNIX System V. Incorporates extensive network connectivity
HFSI XTS-200	TCSEC class B3 - This is a UNIX version of the prior Honeywell SCOMP. It has been noted to have performance problems. It may find its heaviest usage as a guard type device, or low speed server (such as an audit repository).
III. Trusted DBMS	There are several trusted DBMS products at low end (MLS) trust level. High trust DBMS work is seeing some significant activity in Army and Navy R&T programs.
Informix Online/Secure	TCSEC-TDI class B1 -- operates on various versions of UNIX and on VMS
Trusted Oracle 7	TCSEC-TDI class B1 -- operates on various versions of UNIX and on VMS
IV. GUARDs	SUNG, USAFE Guard, GDSS Guard, STATS Guard, AMC WWMCCS Guard, and the EPIC Guard --- Automated upgraders and downgraders, some with man in the loop and some not. Temporary fix solutions -- not mid and long term sufficient.

V. Net Security	Products include direct dial, traditional link KGs (low-to-high speed), LAN security products, and in-line network encryptors (NES, CANEWARE, BLACKER) -- XEUs which were once suitable for some LAN secure communication solutions, have been abandoned completely by Xerox
STU-III	The STU-III fits into the near-term transition as a direct dial solution
Traditional Link KG	Traditional link encryptors fit into the near and mid-term (much less useful in far-term)
Verdix VSLAN/VLANE 5.1	TCSEC-TNI B2 (for Ethernet LAN users)
Motorola NES	COMSEC certified for Type 1 use -- no TCSEC TNI rating
Harris LAN/SX	TCSEC-TNI B1 (goes with Harris
BLACKER	A1, antiquated by net, key management, and Intel 80286 technology (layer 3 INE)
CANEWARE	Designed to be "B2-like," but may be antiquated -- may serve as first version of MISSI INE (layer 3)
Gemini TNP	Trusted Network Processor TCSEC-TNI A1 (various guards use Gemini386 based platform)
Boeing SNS	TCSEC-TNI A1, used as a network interface device -- does not use cryptography
Boeing MLS LAN	TCSEC class A1 (adds management -- proprietary) to SNS already evaluated

Only NES has had a product profile performed on it. Some of these devices have been used in system profiling efforts; results have been eye openers -- there were significant integration problems encountered and system vulnerabilities uncovered.

INFOSEC PRODUCTS *IN THE EVALUATION* PIPELINE
-- A Representative View

PRODUCT CATEGORY	GENERAL DESCRIPTION
I. Workstations & WS-size hosts and servers -- can be used as Guards and Secure Relay Systems	All of the secure workstations are UNIX based -- some have a DOS emulation mode. The general problem with all the workstations is that they do not incorporate network security features, and there are no standard security management features. They can not support multiple simultaneous security policies. They can be made to support multiple information domains, but the isolation of domains is at the low end (B1) level of strength. They do fit into the DGSA transition, but only as near-term transition components. The CMWs may have mid (or even far) term life in the intelligence mission area, particularly with Military Intelligence organizations.
DEC ULTRIX CMW	In evaluation for TCSEC class B1 workstation (UNIX) -- B1+ features
SUN Trusted Solaris	In evaluation for TCSEC class B1 workstation (UNIX) -- B1+ features
Silicon Graphics Trusted IRIX/B	In evaluation for TCSEC class B1 workstation (UNIX) --B1+ features
SecureWare (SCO)	In evaluation for TCSEC class B1 workstation (SCO UNIX) -- B1+ features
II. HOSTS	All of the workstations under evaluation can also be used as hosts, in addition to the following.
Sequent	In evaluation for TCSEC class B1 (real-time UNIX)
HFSI XTS-300	In evaluation for TCSEC class B3 (next generation SCOMP- runs UNIX)
III. DBMSs	There is one DBMS under evaluation at the low end (B1) of trust.
Sybase	In evaluation for TCSEC TDI B1
IV. GUARDs	There are five Guard devices in for evaluation, to add to the other six currently available. All are scheduled to be out of evaluation by end CY94.
Radiant Mercury	Info TBD
JSIPS Guard	Info TBD
EISI Guard	Info TBD
Ops/Intell Interface	Info TBD (complete eval 4/94)
USCENTCOM WWMCCS Guard	Info TBD (was to complete eval by 3/94)
V. Net Security	There are no products in this category under evaluation at this point in time. These products are strictly COMPUSEC devices - no crypto

The majority of the Guard devices in evaluation satisfy the CINCs upgrade & downgrade needs in an otherwise System High security mode environment. The Gemini TNP is planned for used in the Pentagon, and may migrate to other environments if it works correctly and achieves reasonable performance expectations.

INFOSEC PRODUCTS *IN THE DEVELOPMENT PIPELINE*
-- A Representative View

PRODUCT CATEGORY	GENERAL DESCRIPTION
I. Workstations & WS-size hosts and servers -- can be used as Guards and Secure Relay Systems	All of the secure workstations are UNIX based -- some have a DOS emulation mode. They are generally the same as those under evaluation and those currently available. They can be made to support multiple information domains, but the isolation of domains is at the low end (B1+) level of strength. They do fit into the DGSA transition, but only as near-term transition components. The CMWs may have mid (even far) term life in the intelligence mission area.
Early version WSP	MISSI prototype of Workstation Security Package (WSP) for MOSAIC interface - scheduled availability of WSP production units is now planned for 12/95.
HP CMW	In development for TCSEC class B1 workstation (UNIX) -- B1+ features -- Completion date unknown
Data General DG/UX	In development for TCSEC class B2 (UNIX) - Completion date unknown
2-level workstation	Managed by MLS Program Office - Sun Trusted Solaris w/ Cisco Router on High Side and NSC Router on Low - targeted to B2 level of trust. Completion
Harris	In development for TCSEC Class B2 workstation (UNIX) - completion date unknown
SNS w/MOSAIC	Release 1 of the MISSI SNS w/MOSAIC is for the SMG -- scheduled completion date TBD
SNS - SMTP	MISSI SNS that will support SMTP only -- scheduled completion data TBD
MISSI LAW - SMTP	MISSI Local Authority Workstation prototype (SMTP support only) - scheduled completion 7/95
MISSI LAW -X.400	MISSI Local Authority Workstation production units (X.400 support added) - scheduled completion 12/95
II. HOSTS	All of the workstations under evaluation can also be used as hosts, in addition to the following
SCC	In development for TCSEC class A1 -- MISSI Network Server is based on this technology -- date to enter evaluation pipeline is unknown
TIS's T-Mach	TIS is obtaining funding from both ARPA and MISSI (initially planned to be basis of MISSI WISP secure workstation) -- in development for TCSEC class B3 -- date to enter evaluation pipeline is unknown -- first separation kernel based product
III. Trusted DBMS	There is one trusted relational DBMS product under development at low to medium end (MLS) trust level.
Informix	In development for TCSEC-TDI class B2 (already evaluated at class B1)
IV. GUARDs	There are two Guard devices in development, to add to the other eleven already evaluated and/or in the evaluation pipeline.
Standard Mail Guard	SMG to be based on SCC features -- to be used between Secret and Unclassified System High Mode enclaves to up/downgrade electronic mail (SMTP) -- initial prototype SMG scheduled for completion by 8/94
Std WWMCCS Guard	Info TBD (could be mainstay of early GCCS)
V. Net Security	Here there is a mix of secure messaging, in-line encryptors, narrow band ISDN encryption (the STE), and a secure LAN enhancement device
General Kinetics Secure IP Router	Secure IP LAN device for the General Kinetics (formerly VERDIX) router - in development for TCSEC-TNI class B2
MISSI MOSAIC FORTEZZA	PCMCIA crypto card - scheduled availability - contract limited to max of 72K cards starting at production rate of 2K cards/month in 12/94. Max production capability 12K cards/month

MISSI INE	Early version of In-line Network Encryptor may be CANEWARE CFEs -- Fast-lane program to develop quick turn around 100+ Mbps INEs with ATM interface
MISSI Directory Server	MISSI Directory to support MOSAIC -- scheduled completion date TBD
KG-189 Link Encryptor	High speed SONET link encryptor being developed for range of speeds
ITT SNIU	Targeted for TCSEC -TNI B2 - Protects high-level user enclave from low-level user enclave
NSC Router	Targeted for TCSEC -TNI B1
ACC Stealth Router	Targeted for TCSEC -TNI B1

Note that the production of the MISSI SNS may be the best possible baseline for the Radiant Mercury Guard which is currently in evaluation. It should at least be considered a strong candidate for a migration path. Radiant Mercury at present, for all practical purposes, has no real security features other than physical/procedural controls

INFOSEC PRODUCTS *PLANNED FOR DEVELOPMENT*
-- A Representative View

PRODUCT CATEGORY	GENERAL DESCRIPTION
I. Workstations & Hosts	WSs and Hosts planned for development will be based on separation kernel technology to follow the path industry is taking with micro-kernels. The separation kernel approach should solve many of the problems we currently face with operating system portability and having to re-evaluate every time something changes. With this technology the operating system (or the major portion of it) does not have to be highly trusted -- the underlying bedrock is what is trusted.
MISSI WISP	T-MACH or other candidate B3/A1 components -- this is a MISSI development activity -- RFP to be released end FY94 -- scheduled completion date TBD
MISSI NSMs	Includes an Audit Manager, Re-key Server, MLS Directory, Mail List Agent, and improvements to LAW (as necessary) - RFP to be released end FY94 -- scheduled completion date TBD
MISSI Planned Product Improvements	MISSI plans to make improvements to the SNS and the NSMs: SNS will have more functions (like interactive file transfers); NSMs will add security improvements like a multilevel audit manager capability and improvements to the multi-level directory -- all aspects of a MISSI Release Schedule are nebulous at this time-- detailed planning activities have not yet taken place.
II. HOSTS	All of the workstations planned for development can also be used as hosts. It is anticipated that significant product development planning for Hosts and Workstations will result from the R&T efforts on Distributed Trusted Mach to begin in the near future (out of NSA R2) -- it is at this point where strong DGSA transition technology can be proven (or disproved) in support of multiple simultaneous security policy workstation/host bedrock using the separation kernel approach
III. Trusted DBMS	Only R&T planned activities are known at this time-- no planned development other than those products already in development
IV. GUARDs	There are no known new Guards being planned that are not already under development With thirteen of them either available, in evaluation, or in development, there should be plenty around to fill most voids -- but we should not count on it.
V. Net Security	Here there is a mix of secure messaging, in-line encryptors, narrow band ISDN encryption (the STE), and a secure LAN enhancement device

(This page is intentionally blank.)

APPENDIX B EXAMPLES OF AVAILABLE AND EMERGING STANDARDS APPLICABLE TO THE DGSA

Table B-1. Example of Applicability of Available Standards to the DGSA

TYPE	TITLE	ORGANIZATION	STATUS
General	IS 7498-2, Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture	ISO	IS Feb. 1989 (CCITT X.800)
	CD 10181-5, Security Frameworks for Open Systems: Confidentiality	ISO/IEC JTC1 SC21	IS 1993
	CD 10181-6, Security Frameworks for Open Systems: Integrity	ISO/IEC JTC1 SC21	IS 1994
Management Information Elements	CD 10164-9.2, Information Technology - Open System Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control	ISO/IEC JTC1 SC21	CD 1991 IS Dec. 1992 (CCITT X.741)
	ISO 10165-2: 1991: Definition of Management Information	ISO	
	IS 10165-4: 1991: Guidelines for Definition of Management Information	ISO	
Security Management Protocols	DIS 10736, PDAM1, SC6 N6779, Transport Layer Security Protocol Plus PDAMon Security Association Establishment Protocol	ISO/IEC JTC1 SC6	DIS PDAM1
	IS 9596-1, Common Management Information Protocol (CMIP)	ISO	
	General Upper Layer Security: Security Exchange Service Element Protocol (GULS SESEP)	IEEE	
Key Management Protocols	SDNS KMP, Secure Data Network Systems Key Management Protocol	SDNS	
	Kerberos	MIT Project Athena	de facto standard
	X9.17-1985, Financial Institution Key Management (Wholesale)	ASC X9	reaffirmed 1991

Table B-2. Example of Applicability of Emerging Standards to the DGSA

TYPE	TITLE	ORGANIZATION	PROJECTION
General	CD10181-1, Security Frameworks for Open Systems: Overview	ISO/IEC JTC1 SC21	IS June 1994
	CD 10181-4, Security Frameworks for Open Systems: Non-Repudiation	ISO/IEC JTC1 SC21	IS June 1994
Security Management Protocols	Security Association Management Protocol (SAMP)	IEEE (in development)	Projected as a FIPS Pub
Security Information Objects	JTC1/SC27 N604, N605, and N611, Security Information Objects	ISO/IEC JTC1 SC27	WD Nov. 1992 CD 1993 DIS 1994 IS 1995
	IT Security Techniques - Security Information Objects	X3 Project 885	
	Standard Security Label for Government Open Systems Interconnection Profile (generic)	NIST	Draft FIPS PUB
	MIL-STD-2045-18501, Common Security Label	DOD Draft	MIL-STD - April 1994
Key Management Protocols	IEEE 802.10C, Standard for Interoperable LAN Security - Part C: Key Management	IEEE	Draft Apr. 10, 1992

REFERENCES

[1] Center for Information Systems Security (CISS), 1993, *Technical Architecture Framework for Information Management*, Volume 6: Department of Defense (DOD) Goal Security Architecture, Version 1.0, Defense Information Systems Agency (DISA)

[2] Department of Defense (DISSP), 22 February 1993, *Department of Defense Information Systems Security Policy, DISSP-SP.1*

[3] Center for Information Management (CIM), 1992, *Technical Architecture Framework for Information Management (TAFIM)*, Defense Information Systems Agency, Washington, DC

[4] Department of Defense (DoD), August 1991, *Defense-Wide Information Systems Security Program Action Plan*

[5] _____, 1985, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, Washington, DC

[6] Joint Security Commission Staff, June 1994, *A Blueprint for Redefining Security*

[7] Office of the President, 2 April 1982, Executive Order 12356, National Security Information

[8] Institute of Electrical and Electronic Engineers (IEEE), 1993, Standard for Interoperable LAN/MAN Security, Part 3--Key Management Protocol Specification (Draft), IEEE 802.10c

[9] National Security Agency, MOSAIC Program Office (NSA V332), 28 January 1994, *MOSAIC Program Overview*, Version 2

[10] Chairman, Joint Chiefs of Staff, 12 January 1992, Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior

[11] Perry, William, June 1994, *Specifications & Standards -- A New Way of Doing Business*" Memorandum, Secretary of Defense, Washington, DC

[12] DoD, March 1994, *Survey of Available and Ongoing Security Standards and Products*

[13] National Institute of Standards and Technology (NIST), March 1994, *DGSA Security Standardization Areas*, Version 1.0

[14] _____, May 1994, *A Mapping of Standards and DGSA Standards Requirements*

[15] Joint Security Commission Staff, June 1994, *A Blueprint for Redefining Security*

[16] National Security Telecommunications and Information Systems Security Committee, June 1994, *National Training Standard for Information Systems Security (INFOSEC)*

Professionals, National Security Telecommunications and Information Systems Security Instruction 4011

[17] SPIWG, March 1994, *Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*, draft

[18] Dixon, Frank L., April 1993, briefing, *A Defense Logistics Agency View "Getting Down to Cases" in the C&A Business*, DoD Security Process Improvement Working Group (SPIWG) meeting notes 15 April 93.

[19] National Computer Security Center (NCSC), January 1994, *Introduction to Certification and Accreditation*, NCSC-TG-029, Version 1, Ft. George G. Meade, MD

[20] McCumber, Captain John R., "Application of the Comprehensive INFOSEC Model: Mapping the Canadian Criteria for Systems Certification," USAF, Joint Staff/J6K, The Pentagon, Washington, DC., *Proceedings of the 15th National Computer Security Conference*, October 1992.

[21] Ruiz, Hector , SPIWG Meeting, DISSP Office, 15 April 1993, briefing, DoD Security Process Improvement Working Group (SPIWG) meeting notes 15 April 93.

[22] Defense Information Systems Security Policy Program (DISSP), "Process Improvement Strawman," 14 April 1993, DoD Security Process Improvement Working Group (SPIWG) meeting notes 15 April 93.

[23] National Computer Security Center, May 1993, C&A *Process Handbook*,, draft, Ft. George G. Meade, MD

LIST OF ACRONYMS

A&E	Architecture & Engineering
AIS	Automated Information System
ASD	Assistant Secretary of Defense
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4IFTW	Command, Control, Communications, Computers, and Intelligence for the Warrior
C&A	Certification & Accreditation
CBT	Computer Based Training
CFA	Center for Architecture
CFII	Center for Integration and Interoperability
CFS	Center for Standards
CIA	Central Intelligence Agency
CINCs	Commander in Chiefs
CISMO	
CISS	Center for Information Systems Security
COTS	Commercial-off-the-Shelf
CMW	Compartmented Mode Workstation
CN	Communications Networks
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOP	Concept of Operation
CSL	Computer Systems Laboratory
CY	Calendar Year
DAA	Designated Approving Authority
DACUM	Develop a Curriculum
DARIC	
DBMS	Database Management System
DCI	Director of Central Intelligence
DCIDs	Director of Central Intelligence Directives
DGSA	Department of Defense (DOD) Goal Security Architecture
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN-NT	Defense Information Systems Network (DISN) Near-Term (NT)
DISSP	Defense-Wide Information Systems Security Program
DISSP-SP.1	Defense Information System Security Policy
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Message System
DoD	Department of Defense
DODD	Department of Defense Directive
DOTS	DGSA Overall Transition Strategy
DSAWG	DoD Security Accreditation Working Group

E&T	Education & Training
EC&A	Evaluation, Certification and Accreditation
EKMS	Electronic Key Management System
EO	Executive Order
EPL	Evaluated Products List
FISSEA	Federal Information Systems Security Educator Association
FY	Fiscal Year
GCCS	Global Command and Control System
GG	Global Grid
GOTS	Government Off-the Shelf
GSSAPI	Generic Security Services Application Programming Interface
GUI	Graphical User Interface
I&A	Identification & Authentication
IEEE	Institute of Electrical & Electronic Engineers
IM	Information Management
INFOSEC	Information Systems Security
IP3	INFOSEC Policy, Plans, and Procedures
IR&D	Internal Research & Development
IRM	Information Resource Management
ISO	International Standards Organization
ISSO	Information Systems Security Organization
ISSP	Information System Security Program
ISWG	INFOSEC Standards Working Group
JIEO	Joint Interoperability and Engineering Organization
JSC	Joint Security Commission
JITC	Joint Interoperability Test Center
LAN	Local Area Network
LAW	Local Authority Workstation
LSE	Local Subscriber Environment
MAN	Metropolitan Area Network
MISSI	Multilevel Information System Security Initiative
MILDEPs	Military Departments
MLS	Multilevel Security
MOPs	Military Operational Procedures
NCSC	National Computer Security Center
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NPR	National Performance Review
NSA	National Security Agency
NSM	Network Security Management
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction

OASD	Office of Assistant Secretary of Defense
OPSEC	Operations Security
OSD	Office of the Secretary Defense
P3RM	Plans, Policy, Programs, and Resource Management
PBS	Public Broadcasting System
PCMCIA	Personal Computer Memory Card International Association
PL	Public Law
POM	Program Operation and Maintenance
R&D	Research & Development
R&T	Research & Technology
RFP	Request for Proposal
S2T2	Security Standards Transition Team
SAMP	Security Association Management Protocol
SCC	Standards Coordinating Committee
SECDEF	
SILS	Standard for Interoperable LAN/MAN Security
SM	Security Management
SMAP	Security Management Application Process
SMIB	Security Management Information Base
SMG	SNS Mail Guard
SMTP	Simple Mail Transfer Protocol
SNS	Secure Network Server
SPDF	Security Policy Decision Function
SPEF	Security Policy Enforcement Function
SPIWG	Security Process Improvement Working Group
SPWG	Security Policy Working Group
TAFIM	Technical Architecture Framework for Information Management
TCSEC	Trusted Computer Security Evaluation Criteria
TSCM	Technical Security Countermeasures
TFS	Traffic Flow Security
TPEP	Trusted Products Evaluation Program
TSCM	Technical Security Countermeasures
WAN	Wide Area Network